

AN ARAKELOV-THEORETIC APPROACH TO NAÏVE HEIGHTS ON HYPERELLIPTIC JACOBIANS

DAVID HOLMES

CONTENTS

1. Previous explicit computational work on Néron-Tate heights	2
2. Other algorithms for heights in arbitrary genus	3
2.1. Comparison of the algorithms	4
2.2. Extension to the non-hyperelliptic case	4
3. Notation and choice of a resolution	5
3.1. A regular model	5
4. A theorem of Faltings - Hriljac	6
5. Outline	6
6. Metrics on C	7
7. Non-Archimedean I: the Φ term	8
8. Non-Archimedean II: local comparison of metrics and intersection pairings	9
9. Merkl's Theorem	14
9.1. Statement of the Theorem	14
9.2. Constructing a Merkl atlas	15
9.3. Making the constants in Merkl's theorem explicit	16
10. Theta functions to compute Green's functions	18
10.1. Pseudo-metrics to approximate Green's functions	18
10.2. Some results of de Jong	19
10.3. Proof of Lemma 20	20
10.4. Case 1: not both Weierstrass points	20
10.5. Case 2: p_0 and q_0 both Weierstrass points	24
11. The first naïve height	25
12. Refined naïve heights	27
13. Appendix: an algorithm to compute a cover of the Riemann sphere	35
References	37

We give an Arakelov-theoretic definition of a naïve height on divisors of degree zero on a hyperelliptic curve over a number field, and show that this naïve height has computably bounded difference from the Néron-Tate height of the corresponding point on the Jacobian, a key ingredient being a theorem of Faltings and Hriljac (Theorem 2) comparing the Néron-Tate height on the Jacobian to the arithmetic intersection pairing on the curve.

Date: September 7, 2012.

To simplify the exposition, we restrict to the case where our ground field is \mathbb{Q} .

We then use this result to give a new algorithm to compute the finite set of points on a hyperelliptic Jacobian of Néron-Tate height less than a given bound. This is important for a number of applications, for example to the problem of saturation (see [Sik95] or [Sto02]), to the computation of integral points on hyperelliptic curves (see [BMS⁺08]), to the use of Manin's algorithm [Man71], and for numerically testing cases of the Conjecture of Birch and Swinnerton-Dyer.

This paper bears some resemblance to the final two chapters of the author's PhD thesis [Hol12b]. The author would like to thank Samir Siksek for introducing him to the problem, and also Steffen Müller and Ariyan Javanpeykar for some extremely helpful discussions, as well as very thorough readings of a draft version.

1. PREVIOUS EXPLICIT COMPUTATIONAL WORK ON NÉRON-TATE HEIGHTS

The first definition of the Néron-Tate height was given by Néron in 1965 [Nér65]. The problems of computing the height and computing sets of points of bounded height have been studied since the work of Tate in the 1960s (unpublished), who gave a different definition from Néron which is sometimes easier to work with. Using this definition, Tate (unpublished), Dem'janenko [Dem68], Zimmer [Zim76], Silverman [Sil90] and more recently Cremona, Prickett and Siksek [CPS06] and Uchida [Uch06] have given increasingly refined algorithms in the case of elliptic curves. Meanwhile, in the direction of increasing genus, Flynn and Smart [FS97] gave an algorithm for the above problems in genus 2 building on work of Flynn [Fly93], which was later modified by Stoll ([Sto99] and [Sto02]). Recently, Stoll has announced an extension to genus 3 [Sto12].

The technique used by all these authors was to work with a projective embedding of the Jacobian or a quotient (usually the Kummer variety), together with equations for the duplication maps, and thereby obtain results on heights using Tate's telescoping trick. However, such projective embeddings become extremely hard to compute as the genus grows - for example, the Kummer variety is \mathbb{P}^1 in genus 1, is a quartic hypersurface in \mathbb{P}^3 for genus 2 and in genus 3 is given by a system of one quadric and 34 quartics in \mathbb{P}^7 [Mue10]. As such, it appears that to extend to much higher genus using these techniques will be impractical.

In [Hol12a], the author used techniques from Arakelov theory to give an algorithm to compute the Néron-Tate height of a point on a hyperelliptic curve, and a similar (though different) algorithm for the same problem was given by Müller in [Mue11]. Both gave computation examples in much higher genera (9 and 10 respectively) than had been possible with previous techniques, demonstrating that Arakelov theory can be effectively applied to this situation. This paper is a natural continuation of these ideas.

2. OTHER ALGORITHMS FOR HEIGHTS IN ARBITRARY GENUS

As well as the development of practical algorithms to compute with heights on Jacobians of curves of low genus as described above, there is a parallel story of attempting to give algorithms which are valid for all (or large classes of) curves, though they may not be practical to implement. As with the computational approach, one usually starts by fixing a projective embedding of the Jacobian by a multiple of the theta divisor, and defines the naïve height of a point to be the projective height of the image of that point under the embedding. Combined with bounds on the difference between the naïve and Néron-Tate heights, this could be used to give an algorithm to compute the set of points of Néron-Tate height up to a given bound, and this is the approach that has been adopted by most authors mentioned in the previous section.

It appears that it would be possible to give algorithms for bounding the difference between the Néron-Tate and naïve heights for curves of arbitrary genus using this setup, but to the author's knowledge such algorithms have never been written down. Various authors have worked in this direction, and we mention certain of their contributions before comparing these results to those obtained in this paper using Arakelov theory. We restrict our attention to curves of genus at least 3, since the lower genus cases are covered above.

Firstly, the works of Mumford [Mum66] and Zarhin and Manin [ZM72] describe the structure of the equations for abelian varieties embedded in projective space and the corresponding heights and height differences, respectively. Several papers have been written on giving algorithms to construct 'Mumford style' projective embeddings of Jacobians for curves of arbitrary genus. Most of these are restricted to the hyperelliptic case, for example the paper [VW98] of van Wamelen, and the PhD thesis [Rei72] of Reid, who consider embeddings with respect to 4ϑ . The paper [And02] of Anderson considers non-hyperelliptic curves, but only considers (slightly modified) embeddings with respect to 4ϑ . Van Wamelen explicitly presents an algorithm, but the works of Reid and Anderson appear amenable to creating an algorithm.

The other component needed is a bound on the difference between the Néron-Tate height and the naïve height arising from such an embedding. Such a bound is given by Proposition 9.3 (page 665) in the paper [DP02] of David and Philippon, but requires that the Jacobian be embedded using 16ϑ .

The first consequence of this is that we cannot apply the results given above constructing projective embeddings, and so (to the author's knowledge) it is true to say that no algorithm for computing the set of rational points up to given Néron-Tate height has previously been given, even in the hyperelliptic case. On the other hand, it seems very likely that it would be possible with sufficient work to extend for example the work of Anderson to embeddings with respect to 16ϑ , though the result would be unlikely to be straightforward.

The second consequence of the use of an embedding by 16ϑ in [DP02] is that the resulting algorithm is likely to be difficult to use in practise. Recall that the final step in finding the set of points of bounded Néron-Tate height

is always to search some region of projective space for rational points of naïve height less than some other (related) bound. Using an embedding with respect to 16ϑ requires searching for points in projective space of dimension $16^g - 1$ where g is the genus of the curve, and so to search for points of naïve height up to B will require time $B^{16^g - 1}$.

2.1. Comparison of the algorithms. As discussed above, whilst (to the author’s knowledge) no algorithm has previously been given to compute the number of points of Néron-Tate height up to a given bound, it is possible to make some remarks comparing the efficiency of a hypothetical algorithm based on projective embeddings with the algorithm given in this paper. We will thus assume for now that such a hypothetical ‘projective embedding - based’ algorithm is given, extending [And02] to give an embedding by 16ϑ . Since the algorithm in this paper is only for hyperelliptic curves, we will necessarily restrict also to that case.

2.1.1. Time taken to obtain a bound. It should then be possible to bound the time required to compute a bound on the difference between the naïve and Néron-Tate heights using a projective embedding, though the time required would be likely to be large (consider for example that in practise it has not yet been possible to determine the equations for a projective embedding of the Jacobian of any curve of genus 3, or Kummer variety in genus 4).

In contrast, the algorithm presented in this paper uses at several points algorithms for which it is not possible at present to give bounds on the required run-time. In most cases this should not be too hard to remedy, but the step in Section 10 which finds lower bounds on the values of theta functions on certain compact sets looks extremely hard to control.

2.1.2. The size of the bound obtained. For similar reasons to those given above, it seems very hard to predict the size of the bound given by the algorithm in this paper. For a projective embedding, the bound is given in an explicit way in terms of the height of the image of the zero of the abelian variety under the projective embedding. It would be extremely interesting to know if this could be bounded a-priori.

2.1.3. The search region. Recalling that the final stage of either algorithm is to search for rational points up to a given height in a projective space, we observe that the ‘projective embedding’ approach using 16ϑ requires a search in a projective space of dimension $16^g - 1$, whereas the method in this paper requires a search in projective space of dimension g . The low-genus cases suggest that this search may be the bottleneck of the algorithm, in which case this improvement is likely to be substantial in practise.

2.2. Extension to the non-hyperelliptic case. It is reasonable to ask whether the algorithm given in this paper could be extended to the case of non-hyperelliptic curves. Sections 3-10 go through with relatively little change, the main difference being that a Merkl atlas should be constructed by pulling back along a Belyi map, as in [Jav12]. Section 13 is then redundant. Sections 11 and 12 do not carry through easily to the non-hyperelliptic case. It seems reasonable that it would be possible to obtain similar results

to those in these sections using naïve heights on the image of the curve under the canonical embedding, but no details have been worked out by the author.

3. NOTATION AND CHOICE OF A RESOLUTION

Throughout this paper, unless otherwise specified, C will be a hyperelliptic curve of genus g over a number field K living inside weighted projective space $\mathbb{P}(1, 1, g+1)$ with coordinates x, s, y . In Section 11 we will need to specialise to $K = \mathbb{Q}$, but until then we can work in full generality. We write \mathcal{O}_K for the ring of integers in K . We assume C is defined by $y^2 = f(x, s)$ where $f = \sum_{i=1}^{2g+2} f_i x^i s^{2g+2-i}$ has integral coefficients f_i . We write $X = x/s$, $Y = y/s^{g+1}$, $S = s/x$ and $Y' = y/x^{g+1}$.

Definition 1. *For a number field L , a ‘proper set of absolute values for L ’ is a non-empty set of non-trivial absolute values on L such that the product formula holds. Note that we need absolute values (we do not allow their squares), and so if L is not totally real then a proper ‘set’ of absolute values is in fact not a set but a multi-set; we will ignore this distinction.*

These conditions determine a unique proper set of absolute values for each number field L , and we will denote it M_L . This uniqueness implies that if F/L is a finite extension, $|\cdot|_\nu$ an absolute value on L and $|\cdot|_{\omega_1}, \dots, |\cdot|_{\omega_n}$ the absolute values on F extending ν , then for all $x \in F$ we have (writing $N_{F/L}$ for the norm from F to L):

$$(1) \quad \prod_{i=1}^n |x|_{\omega_i} = |N_{F/L}(x)|_\nu,$$

and for all $x \in L$ that

$$(2) \quad |N_{F/L}(x)|_\nu = |x|_\nu^{[F:L]}.$$

We fix once and for all the following notation:

- M_K a proper set of absolute values of K ;
- M_K^0 the subset of non-Archimedean absolute values of K ;
- M_K^∞ the subset of Archimedean absolute values of K ;
- $\kappa(\nu)$ the residue field at an absolute value $\nu \in M_K^0$.

3.1. A regular model. Let \mathcal{C}_1 denote the Zariski closure of C in $\mathbb{P}_{\mathcal{O}_K}(1, 1, g+1)$. A result of Hironaka, contained in his appendix to [CGO84] (pages 102 and 105) gives us an algorithm to resolve the singularities of \mathcal{C}_1 by a sequence of blowups at closed points and along smooth curves (the latter replacing normalisations); we observe that \mathcal{C}_1 may locally be embedded in $\mathbb{P}_{\mathcal{O}_K}^2$, and so Hironaka’s result can be applied.

We fix once and for all a choice of resolution \mathcal{C} of \mathcal{C}_1 using the algorithm of Hironaka - thus we fix both the model \mathcal{C} and the sequence of blowups used to obtain it. We will not need to assume that \mathcal{C} is the minimal desingularisation of \mathcal{C}_1 . We also choose a component of the special fibre over each non-Archimedean absolute value, in order to fix the normalisation of the function Φ later on. This is of course trivial over absolute values over which the special fibre is integral (for example, good reduction), and in practice will

be supplied by the ‘rational point at infinity’ on the odd-degree curves which we will restrict to in the final section.

We write ι_ν the usual (rational-valued) intersection pairing between divisors over $\nu \in M_K^0$ computed on \mathcal{C} (see [Lan88, IV, §1]).

Given an effective prime divisor D on C , we extend it to a horizontal divisor on \mathcal{C} by taking the flat closure. We extend this to arbitrary divisors on C by linearity, and write \overline{D} for this extension.

4. A THEOREM OF FALTINGS - HRILJAC

We shall make use of the following result which can be found in Lang’s book [Lan88, IV, §2].

Theorem 2. (*Faltings* [Fal84] and *Hriljac* [Hri83]) *Let D be a degree zero divisor on C , and let E be any divisor linearly equivalent to D but with disjoint support. Then the height with respect to the ϑ -divisor of the point on $\text{Jac}(C)$ corresponding to D is given by*

$$\hat{h}_\vartheta([\mathcal{O}(D)]) = - \sum_{\nu \in M_K^0} \log |\kappa(\nu)| \iota_\nu(\overline{D} + \Phi(D), \overline{E}) - \frac{1}{2} \sum_{\nu \in M_K^\infty} g_{D,\nu}(E)$$

where Φ and $g_{D,\nu}$ are defined as follows:

- Φ sends a divisor of degree 0 on the curve C to an element of the group of fibral \mathbb{Q} -divisors on \mathcal{C} with order zero along the irreducible component chosen above, such that for any degree-zero divisor D on C (with Zariski closure \overline{D}) and fibral divisor Y on \mathcal{C} , we have $\iota_\nu(\overline{D} + \Phi(D), Y) = 0$.
- $g_{D,\nu}$ denotes a Green function with respect to the canonical (Arakelov) $(1,1)$ -form for the divisor D , when C is viewed as a complex manifold via the embedding ν (see Section 9.1 for our normalisation of a Green’s function).

5. OUTLINE

Our definition of the height is analogous to the definition of the height of an element x in a number field K as

$$(3) \quad h(x) = \sum_{\nu \in M_K} \log^+ |x|_\nu^{-1}.$$

For each absolute value ν of our number field, we will construct a metric or pseudo-metric d_ν on divisors which measures how far apart they are in the ν -adic topology. We then define

$$(4) \quad \mathcal{H}([D]) = \sum_{\nu \in M_K} \log d_\nu(D, D')^{-1}$$

where D' is a specified divisor which is linearly equivalent to $-D$. Since our curve is compact and our metrics continuous, the function $d_\nu(D, D')^{-1}$ is bounded below uniformly in D , and so we may use \log in place of \log^+ .

After setting up these metrics at non-Archimedean absolute values, we will first show how to bound the difference between the distance between two divisors and their local arithmetic intersection pairing at a non-Archimedean absolute value. This will involve bounding the correction term Φ (see [Lan88, III§3]), and then comparing distances between divisors and lengths of modules, in Section 8. The hardest aspect of this will be allowing for the fact that

the model of C obtained by taking the closure inside projective space over \mathcal{O}_K is not in general a regular scheme, so we must compute precisely how the process of resolving its singularities will affect the intersection pairing.

We then use a theorem of Merkl to construct a weak-pseudo-metric on C at each Archimedean absolute value, and to bound the difference between this function and the local Néron pairing. Finally, we write down two more naïve heights, with successively simpler definitions, each time bounding the difference from the Néron-Tate height. We give an algorithm to compute the number of points of bounded height for the simplest of these naïve heights, completing the algorithm.

6. METRICS ON C

We begin by setting up a collection of metrics.

Definition 3. For each absolute value $\nu \in M_K$, we define $(K_\nu^{alg}, |\cdot|)$ to be an algebraic closure of the completion K_ν together with the norm which restricts to ν on $K \subset K_\nu^{alg}$. For non-Archimedean absolute values ν we define

$$(5) \quad d_\nu : C(K_\nu^{alg}) \times C(K_\nu^{alg}) \rightarrow \mathbb{R}_{>0}$$

by

$$\begin{aligned} & d_\nu((x_p : s_p : y_p), (x_q : s_q : y_q)) \\ &= \begin{cases} \max \left(|x_p/s_p - x_q/s_q|, \left| y_p/s_p^{g+1} - y_q/s_q^{g+1} \right| \right) & \text{if } |x_p| \leq |s_p| \text{ and } |x_q| \leq |s_q| \\ \max \left(|s_p/x_p - s_q/x_q|, \left| y_p/x_p^{g+1} - y_q/x_q^{g+1} \right| \right) & \text{if } |x_p| \geq |s_p| \text{ and } |x_q| \geq |s_q| \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

Proposition 4. For each $\nu \in M_K^0$, $d = d_\nu$ is a metric on $C(K_\nu^{alg})$. Moreover, for each such ν , we have $d_\nu(p, q) \leq 1$ for all p and q .

Proof. Only the triangle inequality is non-obvious. We begin by observing that if $(x : s : y) \in C(K_\nu^{alg})$ then

$$(6) \quad |x| \leq |s| \implies |y| \leq |s|^{g+1}$$

and

$$(7) \quad |x| > |s| \implies |y| \leq |x|^{g+1}.$$

The first implication holds as

$$(8) \quad |y|^2 = \left| \sum_i f_i x^i s^{2g+2-i} \right| \leq \left(\max_i |f_i| \right) |s|^{2g+2} \leq |s|^{2g+2},$$

and the other case is similar. Combining this with the fact that $|\cdot|$ is p-adic, we see for all $p, q \in C(K_\nu^{alg})$ that $d(p, q) \leq 1$.

From now on we proceed case-by-case. Let $p = (x_p, s_p, y_p)$, $q = (x_q, s_q, y_q)$ and $r = (x_r, s_r, y_r)$. Note that the change of coordinates $x \mapsto s$, $s \mapsto x$, $y/s^{g+1} \mapsto y/x^{g+1}$ preserves the metric (replacing f by its reciprocal polynomial). As such, we may assume without loss of generality that $|x_p| \leq |s_p|$.

Case 1: $|x_q| \leq |s_q|$ and $|x_r| \leq |s_r|$. Then

$$\begin{aligned}
 (9) \quad & d(p, q) + d(q, r) \\
 &= \max \left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right|, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right| \right) + \max \left(\left| \frac{x_q}{s_q} - \frac{x_r}{s_r} \right|, \left| \frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}} \right| \right) \\
 &\geq \max \left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right| + \left| \frac{x_q}{s_q} - \frac{x_r}{s_r} \right|, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right| + \left| \frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}} \right| \right) \\
 &\geq d(p, r).
 \end{aligned}$$

Case 2: $|x_q| \leq |s_q|$ and $|x_r| > |s_r|$. If $|x_q| < |s_q|$ then

$$(10) \quad d(p, q) + d(q, r) = d(p, q) + 1 \geq 1 \geq d(p, r),$$

so we may assume $|x_q| = |s_q|$. Now if $|x_p| = |s_p|$ then we are back to Case 1, so assume $|x_p| < |s_p|$. Then since $|\cdot|$ is p-adic, we have $|x_p/s_p - x_q/s_q| = \max(|x_p/s_p|, |x_q/s_q|) = 1$, so

$$\begin{aligned}
 (11) \quad & d(p, q) + d(q, r) \\
 &\geq \max \left(\left| \frac{x_p}{s_p} - \frac{x_q}{s_q} \right| + \left| \frac{x_q}{s_q} - \frac{x_r}{s_r} \right|, \left| \frac{y_p}{s_p^{g+1}} - \frac{y_q}{s_q^{g+1}} \right| + \left| \frac{y_q}{s_q^{g+1}} - \frac{y_r}{s_r^{g+1}} \right| \right) \\
 &\geq 1 \geq d(p, r).
 \end{aligned}$$

Case 3: $|x_q| > |s_q|$ and $|x_r| \leq |s_r|$. If $|x_p| < |s_p|$ then

$$(12) \quad d(p, q) + d(q, r) = 1 + d(q, r) \geq 1 \geq d(p, r),$$

and if $|x_r| < |s_r|$ then

$$(13) \quad d(p, q) + d(q, r) = d(p, q) + 1 \geq 1 \geq d(p, r).$$

Otherwise we are back to Case 1.

Case 4: $|x_q| \geq |s_q|$ and $|x_r| \geq |s_r|$. Interchanging p and r reduces us to the second case. \square

7. NON-ARCHIMEDEAN I: THE Φ TERM

In this section we work locally over a non-Archimedean absolute value, so for the remainder of this section let \mathcal{C} denote a regular model of the curve C over a discrete valuation ring R finite over \mathbb{Z}_p . We replace R by an unramified extension such that all irreducible components of the special fibre of \mathcal{C} over R are geometrically irreducible. If \mathcal{C} is smooth over R , then the constructions in this section are trivial. We will show how to bound the values of the function Φ , as defined in [Lan88, III§3].

Let F denote the free abelian group generated by prime divisors supported on the special fibre, and let V denote the finite-dimensional \mathbb{Q} -vector space obtained by tensoring F over \mathbb{Z} with \mathbb{Q} . Let $M : V \times V \rightarrow \mathbb{Q}$ be the map induced by tensoring the restriction of the intersection pairing on \mathcal{C} to its special fibre with \mathbb{Q} . Then V has a canonical basis of fibral prime divisors, so we may confuse M with its matrix in this basis. Call the basis vectors $Y_1 \dots Y_n$; we use the same labels for the corresponding fibral prime divisors.

We will make use of the Moore-Penrose pseudo-inverse (first defined in [Pen55]) of the matrix M , which we denote M^+ . We do not need the full definition, only existence and the fact that if for any matrix A the linear system $Ax = b$ has any solutions, then a solution is given by $x = A^+b$.

We will also need the definition of a reduced divisor on a hyperelliptic curve:

Definition 5. *We say that a divisor D on C is semi-reduced if it is effective, any Weierstrass point appearing in its support has coefficient 1, and if its support does not contain any pairs of points p, p^- (where p^- denotes the image of p under the hyperelliptic involution). If in addition we have $\deg(D) \leq g$, then we say D is reduced.*

Proposition 6. *Let M^+ denote the Moore-Penrose pseudo-inverse of M , let m_- denote the infimum of the entries of M^+ and m_+ their supremum. Let $D = D_1 - D_2$ and $E = E_1 - E_2$ be differences of reduced divisors on C with no common points in their supports, and assume that D and E both have degree zero. Then*

$$(14) \quad |\iota_\nu(\Phi(D), \overline{E})| \leq g^2(m_+ - m_-).$$

Proof. Let d denote the vector $\sum_{i=1}^n \iota_\nu(\overline{D}, Y_i) Y_i$, and similarly set e to equal $\sum_{i=1}^n \iota_\nu(\overline{E}, Y_i) Y_i$, a pair of vectors in V . Now by definition of Φ we have that for all vectors $v \in V$:

$$(15) \quad v \cdot d^T + v \cdot M \cdot \Phi(D)^T = 0,$$

and hence that

$$(16) \quad d^T = -M \cdot \Phi(D)^T.$$

Using the property of the Moore-Penrose pseudo-inverse given above, we can take $\Phi(D)$ to be $-d \cdot (M^+)^T$, and so we find

$$(17) \quad \iota_\nu(\Phi(D), \overline{E}) = -d \cdot (M^+)^T \cdot e^T.$$

Now since D and E are differences of reduced divisors, d and e are vectors each formed by assigning g copies of ‘+1’ and g copies of ‘-1’ to the basis elements Y_1, \dots, Y_n (allowing multiple ± 1 s to be assigned to a single basis vector), and so the result easily follows. \square

Definition 7. *Using the above proposition, we can define a computable constant \mathcal{B}_1 depending only on \mathcal{C} such that for all differences of reduced divisors D and E with no common points in their supports, we have*

$$(18) \quad \left| \sum_{\nu \in M_K^0} \iota_\nu(\Phi_\nu(D), \overline{E}) \right| \leq \mathcal{B}_1.$$

8. NON-ARCHIMEDEAN II: LOCAL COMPARISON OF METRICS AND INTERSECTION PAIRINGS

We compare the metrics and intersection pairing for points on C . The main difficulty is that of working with regular models for C ; the naïve projective closure of the generic fibre is not in general regular, but rather must be modified by a sequence of blowups at smooth centres to obtain a regular

model. We must determine how these modifications will affect the intersection numbers, and also keep careful track of the base field since regular models are not in general stable under ramified base change.

Let b denote the longest length of a chain of blowups involved in obtaining \mathcal{C} from \mathcal{C}_1 (one blowup is considered to follow another if the centre of one blowup is contained in the exceptional locus of the previous one). This is finite since Hironaka's algorithm terminates in a finite number of steps. Note that we fixed a choice of the resolution \mathcal{C} and the algorithm, so that \mathcal{C} and b are well-defined.

Recalling the definition of the metric $d(-, -)$ from Section 6, the aim of this section is the following global result (which will follow easily from the subsequent local results):

Proposition 8. *There exists a computable constant \mathcal{B}_2 such that for all reduced divisors D and E (with no common points in their supports) on C with closures \mathcal{D} and \mathcal{E} on \mathcal{C} , we have*

$$(19) \quad \left| \sum_{\nu \in M_K^0} \iota_\nu(\mathcal{D}, \mathcal{E}) - \frac{1}{[L : K]} \sum_{\nu \in M_L^0} \log^+ \left(\frac{1}{\prod_{i,j} d_\nu(p_i, q_j)} \right) \right| \leq \mathcal{B}_2$$

where L/K is any finite extension over which both D and E have pointwise rational support.

Proof. This is a global version of Proposition 9, whose validity we shall assume for now. We begin by noting that there are only finitely many absolute values of bad reduction for K , and that at any absolute value ν of K of good reduction, we have

$$(20) \quad \left| \sum_{\omega|\nu} \iota_\omega(\mathcal{D}, \mathcal{E}) - \frac{1}{[L : K]} \sum_{\omega|\nu} \log^+ \left(\frac{1}{\prod_{i,j} d_\omega(p_i, q_j)} \right) \right| = 0$$

by applying Proposition 9 in the case $b_\nu = 0$.

As such, it suffices to fix a absolute value ν of K , and then bound the quantity

$$(21) \quad \left| \sum_{\omega|\nu} \iota_\omega(\mathcal{D}, \mathcal{E}) - \frac{1}{[L : K]} \sum_{\omega|\nu} \log^+ \left(\frac{1}{\prod_{i,j} d_\omega(p_i, q_j)} \right) \right|$$

(where the sums are over absolute values ω of L dividing ν) uniformly in D , E and L . We begin by noting that the expression does not depend on the choice of L . Now $L \otimes_K K_\nu$ is a product of finite extensions of the completion K_ν , and moreover the degree and number of the extensions may be bounded in terms of the genus g of C . We may then apply Proposition 9 to each of these fields to obtain the result. \square

The remainder of this section will be given over to stating and proving the local result Proposition 9. For this, we fix a non-Archimedean absolute value ν of K . By base change, we have a chosen resolution \mathcal{C}_{K_ν} of the closure of C in weighted projective space over \mathcal{O}_{K_ν} . Let b_ν denote the longest length of a chain of blowups involved in obtaining this resolution (one blowup is considered to follow another if the centre of one blowup is contained in

the exceptional locus of the previous one) This is finite since Hironaka's algorithm terminates in a finite number of steps. Note that $b_\nu = 0$ if \mathcal{C}_1 is smooth over \mathcal{O}_{K_ν} .

For the remainder of this section, let D and E be effective divisors on C with disjoint support, of degrees d and e respectively. Let L_ν/K_ν be a finite extension of degree m with residue field l such that D and E are both pointwise rational over L_ν . Write $D = \sum_{i=1}^d p_i$ and $E = \sum_{i=1}^e q_i$. Write ω for the maximal ideal of \mathcal{O}_{L_ν} .

Proposition 9. *Let \mathcal{D} and \mathcal{E} denote the Zariski closures of D and E respectively on the regular model \mathcal{C}_{K_ν} over \mathcal{O}_{K_ν} . Then*

$$(22) \quad -b_\nu de \leq \iota_\nu(\mathcal{D}, \mathcal{E}) - \frac{1}{[L_\nu : K_\nu]} \log^+ \left(\frac{1}{\prod_{i,j} d(p_i, q_j)} \right) \leq 0.$$

To avoid an excess of notation, we will from now on drop the subscript ν from the fields and models we are considering - no confusion should result, since we will exclusively be working locally.

To prove Proposition 9, we will need a sequence of lemmas:

Lemma 10. *Let $p \neq q \in C(L) = \text{Hom}_L(L, C_L)$. Write*

$$(23) \quad I_{p,q} \stackrel{\text{def}}{=} \sum_{\Omega|\omega} \log(\#\kappa(\Omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right),$$

where the sum is over closed points Ω of $\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ lying over ω , and I_p and I_q are defining ideal sheaves for the closures in $\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ of the images of p and q in $C \times_K L$. Then

$$(24) \quad I_{p,q} = m \log \left(\frac{1}{d(p, q)} \right).$$

Proof. Write $p = (x_p : s_p : y_p)$, $q = (x_q : s_q : y_q)$ with $x_p, s_p, x_q, s_q \in \mathcal{O}_L$. If $|x_p| < |s_p|$ and $|x_q| > |s_q|$ or vice versa, then \bar{p} and \bar{q} do not meet on the special fibre so $\iota_\omega(\bar{p}, \bar{q}) = 0$, and by definition we see that $d_P(p, q) = 1$.

Otherwise, possibly after changing coordinates, we may assume that p and q are of the form $(x_p : 1 : y_p)$ and $(x_q : 1 : y_q)$ respectively, for $x_p, y_p, x_q, y_q \in \mathcal{O}_L$. Writing F for the (integral) defining equation of C on the coordinate chart containing p and q , and taking Ω to be the closed point where \bar{p} and \bar{q} meet, we have

$$(25) \quad \begin{aligned} \frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} &\cong \frac{\mathcal{O}_L[x, y]_{(x, y)}}{(F, x - x_p, y - y_p, x - x_q, y - y_q)} \\ &\cong \frac{\mathcal{O}_L}{(x_p - x_q, y_p - y_q)}, \end{aligned}$$

so

$$(26) \quad \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right) = \min(\text{ord}_\omega(x_p - x_q), \text{ord}_\omega(y_p - y_q)).$$

Now given $a \in L$, we find

$$(27) \quad \log(\#l) \text{ord}_\omega(a) = -m \log |a|,$$

so

$$(28) \quad \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L, \Omega}}{I_p + I_q} \right) = m \frac{\min(-\log |x_p - x_q|, -\log |y_p - y_q|)}{\log(\#l)},$$

and hence

$$(29) \quad I_{p,q} = m \min(-\log |x_p - x_q|, -\log |y_p - y_q|).$$

However,

$$(30) \quad \log(1/d(p, q)) = \min(-\log |x_p - x_q|, -\log |y_p - y_q|),$$

so we are done. \square

Lemma 11. *Recalling that over L we can write $D = \sum_{i=1}^d p_i$ and $E = \sum_{i=1}^e q_i$, we define $\omega_{i,j}$ to be the closed point of $\mathcal{C}_1 \times_{\mathcal{O}_K} \mathcal{O}_L$ where p_i meets q_j if such exists, and the unit ideal otherwise. Letting \mathcal{I}_D and \mathcal{I}_E denote the ideal sheaves of the closures of D and E respectively on \mathcal{C}_1 , we have*

$$(31) \quad \sum_{i,j} \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\omega_{i,j}}}{I_{p_i} + I_{q_j}} \right) = \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1} \otimes_{\mathcal{O}_K} \mathcal{O}_L}{(\mathcal{I}_D + \mathcal{I}_E) \otimes_{\mathcal{O}_K} \mathcal{O}_L} \right).$$

The analogous statement on \mathcal{C} also holds.

Proof. We may decompose \mathcal{I}_D and \mathcal{I}_E into iterated extensions of the sheaves I_{p_i} and I_{q_i} , whereupon the result follows from additivity of lengths in exact sequences. \square

Lemma 12. *Let \mathcal{I}_D and \mathcal{I}_E denote the ideal sheaves on \mathcal{C}_1 corresponding to the closures of the divisors D and E respectively.*

$$(32) \quad \text{length}_{\mathcal{O}_K} \left(\frac{\mathcal{O}_{\mathcal{C}_1}}{\mathcal{I}_D + \mathcal{I}_E} \right) \cdot \text{ram. deg } L/K = \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_1} \otimes_{\mathcal{O}_K} \mathcal{O}_L}{(\mathcal{I}_D + \mathcal{I}_E) \otimes_{\mathcal{O}_K} \mathcal{O}_L} \right).$$

The analogous statement on \mathcal{C} also holds.

Proof. Let M be a finite length \mathcal{O}_K -module. We show

$$(33) \quad \text{length}_{\mathcal{O}_K}(M) \cdot \text{ram. deg}(L/K) = \text{length}_{\mathcal{O}_L}(M \otimes_{\mathcal{O}_K} \mathcal{O}_L).$$

Let $M = M_0 \subset M_1 \subset \cdots \subset M_l = 0$ be a composition series for M , so each M_i/M_{i+1} is simple. Since \mathcal{O}_K is local, we have by [Mat80, p12] that

$$(34) \quad M_i/M_{i+1} \cong \mathcal{O}_K/\mathfrak{m}_K.$$

By additivity of lengths, it suffices to show

$$(35) \quad \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_K}{\mathfrak{m}_K} \otimes_{\mathcal{O}_K} \mathcal{O}_L \right) = \text{ram. deg}(L/K),$$

but this is clear since $\mathfrak{m}_K \cdot \mathcal{O}_L = \mathfrak{m}_L^{\text{ram. deg}(L/K)}$. \square

Lemma 13. *Let $\phi : \mathcal{C}_3 \rightarrow \mathcal{C}_2$ be one of the blowups involved in obtaining \mathcal{C} from \mathcal{C}_1 . Let $p \neq q \in C_L(L)$. Then*

$$(36) \quad 0 \leq \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_2 \times \mathcal{O}_L}}{I_{\bar{p}} + I_{\bar{q}}} \right) - \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{C}_3 \times \mathcal{O}_L}}{I_{\bar{p}} + I_{\bar{q}}} \right) \leq \text{ram. deg}(L/K).$$

Proof. In this proof, we will omit the subscripts ' \mathcal{O}_L ' from the lengths, since all lengths will be taken as \mathcal{O}_L -modules. If \bar{p} does not meet \bar{q} on $\mathcal{C}_2 \times \mathcal{O}_L$ then both the lengths are zero, so we are done. Otherwise, let Ω be the closed point on $\mathcal{C}_2 \times \mathcal{O}_L$ where \bar{p} meets \bar{q} , and let α be the closed point of \mathcal{C}_2 such that Ω lies over α .

Let R denote the local ring of the (three-dimensional) ambient space to \mathcal{C}_2 at α , and similarly let A be the local ring of \mathcal{C}_2 at α . Let $B \subset R$ be the centre of the localisation of ϕ at α . After étale base-change, we may assume that we have

$$(37) \quad R = \tilde{\mathcal{O}}_K[[x, y]]_{(x, y, a)}$$

where $\tilde{\mathcal{O}}_K$ is finite étale over \mathcal{O}_K and a is a uniformiser in $\tilde{\mathcal{O}}_K$, and that

$$(38) \quad B = (x, y, a) \quad \text{or} \quad B = (x, a),$$

depending on whether we are blowing up a point or a smooth fibral curve.

Blowups commute with flat base change, and the strict transform of a closed subscheme under a blowup is the corresponding blowup of that closed subscheme (see [Liu02, Corollary 8.1.17]), so we can be relaxed with our notation. We may write

$$(39) \quad p = (x - ax_p, y - ay_p) \quad q = (x - ax_q, y - ay_q)$$

where x_p, y_p, x_q and y_q are in $\mathcal{O}_L \cdot \tilde{\mathcal{O}}_K$. Setting ω' to be a uniformiser in the maximal ideal of $\tilde{\mathcal{O}}_K \cdot \mathcal{O}_L$, we have

$$(40) \quad \text{length} \left(\frac{\mathcal{O}_{\mathcal{C}_2 \times \mathcal{O}_L}}{I_p + I_q} \right) = \min(\text{ord}_{\omega'}(ax_p - ax_q), \text{ord}_{\omega'}(ay_p - ay_q)).$$

In the case $B = (x, y, a)$ we look at the affine patch of the blowup given by setting $a \neq 0$; the equations for p and q transform into

$$(41) \quad p' = (x - x_p, y - y_p) \quad \text{and} \quad q' = (x - x_q, y - y_q),$$

so

$$(42) \quad \begin{aligned} \text{length} \left(\frac{\mathcal{O}_{\mathcal{C}_3 \times \mathcal{O}_L}}{I_p + I_q} \right) &= \min(\text{ord}_{\omega'}(x_p - x_q), \text{ord}_{\omega'}(y_p - y_q)) \\ &= \text{length} \left(\frac{\mathcal{O}_{\mathcal{C}_2 \times \mathcal{O}_L}}{I_p + I_q} \right) - \text{ord}_{\omega'}(a). \end{aligned}$$

In the case $B = (x, a)$ we look again at the affine patch of the blowup given by setting $a \neq 0$; the equations for p and q transform into

$$(43) \quad p' = (x - x_p, y - ay_p) \quad \text{and} \quad q' = (x - x_q, y - ay_q),$$

so

$$(44) \quad \begin{aligned} \text{length} \left(\frac{\mathcal{O}_{\mathcal{C}_3 \times \mathcal{O}_L}}{I_p + I_q} \right) &= \min(\text{ord}_{\omega'}(x_p - x_q), \text{ord}_{\omega'}(ay_p - ay_q)) \\ &= \text{length} \left(\frac{\mathcal{O}_{\mathcal{C}_2 \times \mathcal{O}_L}}{I_p + I_q} \right) - (0 \text{ or } 1) \text{ord}_{\omega'}(a), \end{aligned}$$

so the result follows from the fact that, since $\tilde{\mathcal{O}}_K$ is unramified over \mathcal{O}_K , we have

$$(45) \quad \text{ord}_{\omega'}(a) = \text{ram. deg}(L \cdot \tilde{K}/\tilde{K}) = \text{ram. deg}(L/K).$$

□

Proof of Proposition 9. To prove Proposition 9, we apply Lemmata 10, 13, 11 and 12 in that order to find that there exists $0 \leq \beta \leq bde$ such that

$$\begin{aligned}
 (46) \quad \sum_{i,j} \log \left(\frac{1}{d(p_i, q_j)} \right) &= \frac{1}{m} \sum_{i,j} \sum_{\Omega|v} \log(\#\kappa(\Omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{E}_1 \times \mathcal{O}_K \mathcal{O}_L, \Omega}}{I_p + I_q} \right) \\
 &= \frac{1}{m} \sum_{i,j} \sum_{\Omega|v} \log(\#\kappa(\Omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{E} \times \mathcal{O}_K \mathcal{O}_L, \Omega}}{I_p + I_q} \right) + \beta \\
 &= \frac{1}{m} \log(\#\kappa(\omega)) \text{length}_{\mathcal{O}_L} \left(\frac{\mathcal{O}_{\mathcal{E} \times \mathcal{O}_L}}{I_D + I_E} \right) + \beta \\
 &= \frac{1}{m} \log(\#\kappa(\omega)) \text{length}_{\mathcal{O}_K} \left(\frac{\mathcal{O}_{\mathcal{E}}}{I_D + I_E} \right) \cdot \text{ram. deg}(L/K) + \beta \\
 &= \iota_v(\mathcal{D}, \mathcal{E}) + \beta.
 \end{aligned}$$

□

Remark 14. Note that $\beta = 0$ for all but finitely many absolute values v .

9. MERKL'S THEOREM

There are two key tools which we will need to handle local heights at Archimedean absolute values. The first is a theorem of Merkl, and the second is a formula of de Jong taken from his PhD thesis. In this section we will state Merkl's theorem [CE⁺11], along with improvements due to Peter Bruin [Bru06].

9.1. Statement of the Theorem. Let X be a compact connected Riemann surface of positive genus and let μ denote the canonical (Arakelov) (1,1)-form μ on X . We write $g(-, -)$ for the Green's function on $X \times X$ associated to μ , and $G : X \times X \rightarrow \mathbb{R}_{\geq 0}$ for its exponential, which we normalise to satisfy the following three properties:

1) $G(p, q)$ is a smooth function on $X \times X$ and vanishes only at the diagonal. For a fixed $p \in X$, an open neighbourhood U of p and a local coordinate z on U we can write

$$(47) \quad \log G(p, q) = \log |z(q)| + \alpha(q)$$

for $p \neq q \in U$, with α a smooth function

2) for all $p \in X$ we have $\partial_q \bar{\partial}_q \log G(p, q)^2 = 2\pi i \mu(q)$ for $q \neq p$.

3) for all $p \in X$, we have

$$(48) \quad \int_X \log G(p, q) \mu(q) = 0.$$

We give a trivially modified version of the definition of a Merkl atlas which will be more convenient for our purposes - the usual version has $r_1 = r_2$, but the additional data we associate will be useful later on:

Definition 15 (Merkl atlas). A Merkl atlas for X is a quadruple

$$(49) \quad (\{U_j, z_j\}_{j=1}^n, r_1, r_2, M, c_1),$$

where $\{(U_j, z_j)\}_{j=1}^n$ is a finite atlas for X , and $1/2 < r_2 < r_1 < 1$, $M \geq 1$ and $c_1 > 0$ are real numbers such that the following properties hold:

- 1) Each $z_j(U_j)$ is the open unit disc.
- 2) The open sets $U_j^{r_2} \stackrel{\text{def}}{=} \{x \in U_j : |z_j(x)| < r_2\}$ with $1 \leq j \leq n$ cover X .
- 3) For all $1 \leq j, j' \leq n$, the function $|dz_j/dz_{j'}|$ on $U_j \cap U_{j'}$ is bounded from above by M .
- 4) For $1 \leq j \leq n$, write $\mu = iF_j dz_j \wedge d\bar{z}_j$ on U_j . Then $0 \leq F_j(z) \leq c_1$ for all $z \in U_j$.

Theorem 16. Let $\mathbb{M} = (\{U_j, z_j\}_{j=1}^n, r_1, r_2, M, c_1)$ be a Merkl atlas for X . Set

$$(50) \quad \mathcal{B}(\mathbb{M}) = \frac{330n}{(1-r_1)^{3/2}} \log \frac{1}{1-r_1} + 13.2nc_1 + (n-1) \log M.$$

Then

$$(51) \quad \sup_{(p,q) \in X \times X \setminus \Delta} g(p, q) \leq \mathcal{B}(\mathbb{M}).$$

Moreover, for every $1 \leq j \leq n$ and $p \neq q \in U_j^{r_1}$, we have

$$(52) \quad |g(p, q) - \log |z_j(p) - z_j(q)|| \leq \mathcal{B}(\mathbb{M}).$$

Proof. The usual version of the Theorem has $r_1 = r_2$, but the proof of this version follows trivially from the usual one. Merkl proved a less explicit version of this theorem in [CE⁺11, Chapter 10]. A version similar to this was given by Peter Bruin in his Masters Thesis [Bru06, Theorem 3.1], and the result in precisely this form is proven in Bruin's appendix to [Jav12]. \square

9.2. Constructing a Merkl atlas. For the remainder of the section, we fix a complex absolute value of our ground field K , so that we may by slight abuse of notation view a smooth variety over K as a complex manifold.

We will need to explicitly compute the constant $\mathcal{B}(\mathbb{M})$ for our hyperelliptic curve C . In order to do this, we must first fix a construction of a Merkl atlas for C , which we do using ideas from [Jav12]. Recall that we write $\pi : C \rightarrow \mathbb{P}^1$ for the projection map. We will construct an atlas on \mathbb{P}^1 , then lift it to an atlas for C .

9.2.1. An atlas for \mathbb{P}^1 . We first construct a finite cover of the Riemann sphere as a metric space (with the chordal metric) by open discs with the property that for any two such disks D_1 and D_2 , if D_1 contains the centre of D_2 , then $D_1 = D_2$. An algorithm to achieve this is given in Appendix 13.

Next we need to relate this topological cover to a holomorphic cover. We do this one disk at a time;

Definition 17. given a disk D with centre p , translate p to $(0 : 1) \in \mathbb{P}_{x,s}^1$ using a unitary transformation. Then set $z_D(q) = x(q)/|x(q_0)|$ for any q_0 lying on the boundary of D . We set $R = |x(q_0)|$ for any q_0 on the boundary of D . Set $r_2 = |q_1|$ where q_1 is any point in D lying at distance r from p in the chordal metric, and pick any $r_2 \leq r_1 < 1$.

Because of the way we set up this cover of \mathbb{P}^1 , it should be clear that it satisfies the criteria (1), (2) and (3) in the definition of a Merkl atlas.

However, unsurprisingly our real interest lies in constructing a Merkl atlas for C , which we will achieve by lifting this atlas for \mathbb{P}^1 .

9.2.2. Lifting to a Merkl atlas for C . There are two cases to consider in lifting disks D from \mathcal{U} to C . The first and easiest is when D is not centred at (and therefore does not contain) a branch point. Then the preimage $\pi^{-1}(D)$ is a pair of disjoint open sets U_1, U_2 in C (since π is étale outside B), and we take these open sets together with the maps $z_U = z_D \circ \pi$ obtained by composing the projection to \mathbb{P}^1 with the map $z_D : U \rightarrow \mathbb{C}$.

The harder case arises when D contains (and so is centered at) a branch point b . Writing $B_0(1)$ for the unit disk in \mathbb{C} , we take the unique map z making the following diagram commute:

$$\begin{array}{ccc} \pi^{-1}(D) & \xrightarrow{z} & B_0(1) \\ \downarrow \pi & & \downarrow x \mapsto x^2 \\ D & \xrightarrow{z_D} & B_0(1) \end{array}$$

9.3. Making the constants in Merkl's theorem explicit. Now that we have shown how to construct a Merkl atlas, we need to show how to explicitly compute the real numbers M and c_1 appearing in the statement of Merkl's theorem.

9.3.1. The computation of M . It suffices to give an algorithm to find an upper bound on $|\mathrm{d} z_i / \mathrm{d} z_j|$ on $D_i \cap D_j$ for fixed charts (D_i, z_i) and (D_j, z_j) in the Merkl atlas. If neither D_i nor D_j contains a Weierstrass point, write p_i and p_j for their centres. Then

$$(53) \quad z_i(X) = \frac{X - X_{p_i}}{X \overline{X_{p_i}} + 1},$$

and so differentiating we find

$$(54) \quad \frac{\mathrm{d} z_i}{\mathrm{d} z_j} = \frac{|X_{p_i}|^2 + 1}{|X_{p_j}|^2 + 1} \left| \frac{X \overline{X_{p_j}} + 1}{X \overline{X_{p_i}} + 1} \right|^2,$$

so to find a bound on the absolute value of the derivative $\mathrm{d} z_i / \mathrm{d} z_j$ on $D_i \cap D_j$, it suffices to bound this rational function on the domain

$$(55) \quad \{X \in \mathbb{C} : |M_i X| \leq R \text{ and } |M_j X| \leq R\},$$

where

$$(56) \quad M_i = \begin{pmatrix} 1 & -X_{p_i} \\ -\overline{X_{p_i}} & 1 \end{pmatrix}$$

is the unitary matrix translating p_i to $X = 0$, and R is as in Definition 17.

By our construction, at most one of D_i and D_j can contain a Weierstrass point if $D_i \cap D_j$ is non-empty. In this case, we assume without loss of generality that D_i contains the Weierstrass point, and we use a unitary transformation to move its centre p_i to $X = 0$. We proceed in a similar manner to before, using the above descriptions of the matrices M_i and M_j . z_i and z_j are the coordinates on the charts D_i and D_j given in Section 9.2.2

(so z_j is in effect the same coordinate as before, but z_i is the square-root of the coordinate z_i used in the previous case). Differentiating, we obtain

$$(57) \quad \frac{dz_i}{dz_j} = -\frac{1}{2} \frac{|X_{p_i}|^2 + 1}{|X_{p_j}|^2 + 1} \frac{(X\overline{X_{p_j}} + 1)^2}{(X\overline{X_{p_i}} + 1)^{3/4}} \frac{1}{X - X_{p_i}},$$

whose absolute value we bound on the same domain as before.

9.3.2. The computation of c_1 . Since we may translate any Merkl chart to be centred at $X = 0$ using a unitary matrix, we will treat just this case. We may thus write our chart $U = \{(X, Y) \in C : |X| < R\}$ and $z = X/R$ or $z = \sqrt{X/R}$, depending on whether U contains a Weierstrass point. We know that a basis of differential forms on C is given by

$$(58) \quad \frac{X^n dX}{Y} \quad 0 \leq n \leq g-1.$$

Petersson inner products may be computed to any required precision by numerical integration (though care must be taken to either bound the derivatives, use interval arithmetic or similar in order to yield a provably correct result), and applying Gram-Schmidt so we can express the Arakelov $(1, 1)$ form in terms of this basis. It thus suffices to bound the functions $F_{m,n}$ defined by

$$(59) \quad \frac{X^m dX}{Y} \wedge \frac{\overline{X^n dX}}{Y} = F_{m,n} dz \wedge d\bar{z}.$$

We consider first the case where U does not contain a Weierstrass point. Then

$$(60) \quad dz \wedge d\bar{z} = \frac{1}{R^2} dX \wedge d\overline{X},$$

so

$$(61) \quad F_{m,n} = \frac{R^2 X^m \overline{X^n}}{|Y|^2},$$

which is bounded on U .

If U contains (and so is centred at) a Weierstrass point, we have $z = \sqrt{X/R}$, so

$$(62) \quad dz \wedge d\bar{z} = \frac{1}{4|z|^2 R^2} dX \wedge d\overline{X} = \frac{R}{4|X|} dX \wedge d\overline{X},$$

so

$$(63) \quad F_{m,n} = \frac{4|X|}{R} \frac{X^m \overline{X^n}}{|Y|^2}.$$

Now since $Y^2 = F(X) = XF_0(X)$, this reduces to

$$(64) \quad F_{m,n} = \frac{4}{R} \frac{X^m \overline{X^n}}{|F_0(X)|},$$

which is bounded on U .

10. THETA FUNCTIONS TO COMPUTE GREEN'S FUNCTIONS

The formulae and bounds given for Green's functions in the previous section only apply to pairs of points on C which are sufficiently close together - more precisely, to pairs of points which can be contained in the same chart of our Merkl atlas (more precisely, in U^{r_1} where U is a chart). To handle the remaining points, we will use a formula from the thesis of Robin de Jong ([dJ04] and [DJ05]), which expresses Green's functions in terms of theta functions. In order to give uniform bounds, we will use this formula first to evaluate the Green's function at a finite set of pairs of points, and then to bound its derivative so as to obtain bounds for points nearby. C will be a hyperelliptic curve of genus g (though de Jong's results apply to general Riemann surfaces).

10.1. Pseudo-metrics to approximate Green's functions. In order to effectively use de Jong's results on theta functions, and to combine them with the bounds given by Merkl's theorem, we will need to define a weak-pseudo-metric d on points of C such that $\log(d(p_1, p_2))$ is 'not too far from a Green's function'. This function d is analogous to the metrics d_ν given for non-Archimedean absolute values ν , and it will be combined with them in the definition of the naïve height.

We wish to be able to use Merkl's Theorem to show that our weak-pseudo-metric is close to a Green's function for points that are 'close together', and also to be able to apply results with theta functions to show that our weak-pseudo-metric is close to a Green's function for points that are 'far apart'. To enable this, we begin with a rather contrived definition of a weak-pseudo-metric.

Definition 18. Let \mathbb{M} be a Merkl atlas for a hyperelliptic curve C constructed as above and with $r_2 < r_1$. Let $0 < \rho < (r_1 - r_2)/4$, and let \mathcal{V}' be a finite cover of \mathbb{P}^1 by closed disks of radius ρ in the chordal metric, with the property that if any disk contains a branch point then it is centred at that branch point. Lift \mathcal{V}' to a cover \mathcal{V} of C just as we did to obtain the Merkl atlas.

Given two charts V_1, V_2 in \mathcal{V} with centres q_1, q_2 respectively, define $d(V_1, V_2) = G(q_1, q_2)$ (where G is the exponential Green's function) if $V_1 \cap V_2 = \emptyset$, and $d(V_1, V_2) = \infty$ otherwise.

Given two pairs $(p_j, U_j^{r_2})$ with U_j a chart from \mathbb{M} and $p_j \in U_j^{r_2}$, define

$$(65) \quad d((p_1, U_1), (p_2, U_2)) = \begin{cases} |z_1(p_1) - z_1(p_2)| & \text{if } U_1 = U_2 \\ \infty & \text{otherwise} \end{cases}$$

Given two triples (p_j, U_j, V_j) with $p_j \in U_j^{r_2}$, $p_j \in V_j$, U_j a chart from the Merkl atlas \mathbb{M} and V_j a chart from the cover \mathcal{V} , we define

$$(66) \quad d((p_1, U_1, V_1), (p_2, U_2, V_2)) = \min(d((p_1, U_1), (p_2, U_2)), d(V_1, V_2))$$

Given two points $p_1, p_2 \in C$, we define

$$(67) \quad d(p_1, p_2) = \min_{U_1, U_2, V_1, V_2} d((p_1, U_1, V_1), (p_2, U_2, V_2)),$$

where the minimum is taken over all charts U_1, U_2, V_1, V_2 such that $p_j \in U_j^{r_2} \cap V_j$ as before.

It is clear that the function d will depend on the choice of ρ and also on the choice of the cover \mathcal{V} . We will sometimes write d_ρ or $'dd_{\rho,\mathcal{V}}$ when it is important to make this explicit.

Lemma 19. *For all $0 < \rho < (r_1 - r_2)/4$, the function $d_\rho : C \times C \rightarrow \mathbb{R}_{>0} \cup \{\infty\}$ takes finite values.*

Proof. It suffices to show that for every p_1, p_2 , we have either

- 1) there exists a chart $U \in \mathbb{M}$ such that $p_1 \in U^{r_2}$ and $p_2 \in U^{r_2}$.
- 2) There exist disjoint $V_1, V_2 \in \mathcal{V}$ such that $p_1 \in V_1$ and $p_2 \in V_2$.

Suppose (2) fails. Since the V cover C , there must exist a pair of overlapping charts $V, V' \in \mathcal{V}$ such that $p_1 \in V$ and $p_2 \in V'$. In particular, in the chordal metric on \mathbb{P}^1 we find $d(\pi(p_1), \pi(p_2)) \leq r_1 - r_2$. Since the U^{r_2} cover C , there exists a $U \in \mathcal{U}$ such that $p_1 \in U^{r_2}$. Since the chordal distance $d(\pi(p_1), \pi(p_2)) \leq r_1 - r_2$, we see $\pi(p_2) \in \pi(U^{r_1})$. Now if U is a chart containing a Weierstrass point it is clear that $p_2 \in U^{r_1}$, and if not then since the p_j are contained in overlapping charts V , we see again that $p_2 \in U^{r_1}$. \square

The aim of the remainder of this section is to prove the following result:

Lemma 20. *For all $p_1, p_2 \in C$, and for all $0 < \rho < (r_1 - r_2)/4$, we have*

$$(68) \quad |\log d_\rho(p_1, p_2) - g(p_1, p_2)| \leq \max(\mathcal{B}(\mathbb{M}), c(\rho)),$$

where the constant $c(\rho)$ is as defined in Proposition 25.

Definition 21. *To ease the notation, we will from now on fix once and for all a Merkl Atlas, a constant $0 < \rho < (r_1 - r_2)/4$ and cover \mathcal{V} .*

We can then define a constant $\mathcal{B}_3 \stackrel{\text{def}}{=} \max(\mathcal{B}(\mathbb{M}), c(\rho))$, for use later on.

The idea of the proof is as follows:

firstly, if we are in situation (1) of the proof of Lemma 19, then the bound follows immediately from Merkl's Theorem;

secondly, if we are in situation (2), then we need to bound the difference between the value of the Green's function at the centres of the charts V_j with the value of the Green's function evaluated at any points in those charts. To do this, we bound the derivative of the Green's function via a relationship with theta functions.

10.2. Some results of de Jong. We state the main definitions and results we will need from [dJ04]. We restrict to the hyperelliptic case and genus $g \geq 2$ as this simplifies the statements somewhat, though the results hold more generally. We take a Weierstrass point ∞ of the curve as a base-point for the Abel-Jacobi map α to the analytic Jacobian.

Definition 22 ([dJ04, Proposition 1.4.4]). *Let $\tau \in \mathcal{H}_g$ lie in the Siegel upper half space, and $z \in \mathbb{C}^g$. We then define*

$$(69) \quad \|\vartheta\|(z; \tau) = (\det(\Im(\tau)))^{1/4} \exp(-\pi \Im(z)^t (\Im(\tau))^{-1} \Im(z)) |\vartheta(z; \tau)|.$$

Definition 23 ([dJ04, Definition 2.1.1]). *We define the invariant $S(C)$ by the formula*

$$(70) \quad \log S(C) = - \int_C \log \|\vartheta\| (g\alpha(p) - \alpha(q)) d\alpha(p),$$

where q can be chosen to be any point in C .

We will often need to consider expressions of the form $\|\vartheta\|(g\alpha(p) - \alpha(q))$ for $p, q \in C$, so to make things more readable we will from now on drop the α from the notation.

Theorem 24 ([dJ04, Theorem 2.1.2]). *Let $p, q \in C$ with p not a Weierstrass point. Then*

$$(71) \quad G(p, q)^g = S(C)^{1/g^2} \frac{\|\vartheta\|(gp - q)}{\prod_{w \in W} \|\vartheta\|(gp - w)^{1/g^3}},$$

where $G = \exp(g)$ is the exponential Green's function with respect to the canonical $(1, 1)$ form, and the product in the denominator is over the Weierstrass points of C taken with multiplicities, which are all $g(g-1)/2$ in the hyperelliptic case.

The formula still holds for p a Weierstrass point; in this situation both the numerator and denominator vanish to order $g(g-1)/2$, and we must take the ratio of the leading coefficients of power series expansions about p in the numerator and denominator.

10.3. Proof of Lemma 20. To prove the Lemma, it suffices to show the following:

Proposition 25. *Given $\rho > 0$ as in Definition 18, there exists a constant $c(\rho)$ such that for all pairs of pairs $(p, V_p), (q, V_q)$ with $p \in V_p, q \in V_q, V_p, V_q$ elements of the cover \mathcal{V} , we have*

$$(72) \quad \log |G(p, q)/G(p_0, q_0)| \leq c(\rho),$$

where p_0, q_0 are the centres of V_p and V_q respectively.

The proof of this proposition falls into two cases, depending on whether or not both p_0 and q_0 are Weierstrass points.

10.4. Case 1: not both Weierstrass points. Suppose at least one of p_0 and q_0 is not a Weierstrass point. Since the Green's function is symmetric, we may assume without loss of generality that p_0 is not a Weierstrass point, so both the numerator and denominator of the formula in 24 are non-zero. By continuity of theta functions, we may shrink ρ so that neither the numerator or denominator vanishes on the closed sets V_p and V_q .

Now it is clear that the expression

$$(73) \quad \left| \frac{G(p, q)}{G(p_0, q_0)} \right|^g = \frac{\|\vartheta\|(gp - q) \prod_{w \in W} \|\vartheta\|(gp_0 - w)^{(g-1)/(2g^2)}}{\|\vartheta\|(gp_0 - q_0) \prod_{w \in W} \|\vartheta\|(gp - w)^{(g-1)/(2g^2)}}$$

is bounded away from zero, and so it remains to give an algorithm to find such a bound. We do this by bounding the derivatives of the various quantities involved.

10.4.1. Bounds on hyperelliptic integrals. In order to apply bounds on the derivatives of theta functions to bounding the above expression, it is necessary to understand the local behaviour of the map

$$(74) \quad \alpha : C \rightarrow \mathbb{C}/\Lambda$$

given by hyperelliptic integration. For convenience, we give

- (1) a choice of path from p_0 to p ,
and

- (2) an explicit bound on the resulting value $|\alpha(p_0) - \alpha(p)|$.

We briefly recall the setup of hyperelliptic integration: let $\tilde{\omega}_0 = \frac{dx}{y}, \dots, \tilde{\omega}_{g-1} = \frac{x^{g-1} dx}{y}$ be a basis of differential 1-forms on C , let $\{A_i, B_i : i = 1, \dots, g\}$ be a symplectic homology basis, and let $\{\omega_i = \sum_j c_{i,j} \tilde{\omega}_j : i = 1, \dots, g\}$ be a normalised basis of differential forms such that

$$(75) \quad \int_{A_i} \omega_j = \delta_{i,j}.$$

Let $\Lambda \subset \mathbb{C}^{g \times g}$ be the resulting period matrix. Let $\mathfrak{D} \subset \mathbb{C}^g$ be a fundamental domain, and let $\alpha : C(\mathbb{C}) \rightarrow \mathfrak{D}$ be the map obtained by integrating. α_i will denote its i th component, obtained by integrating ω_i , and similarly we set

$$(76) \quad \tilde{\alpha}_i(z) = \int_{\infty}^z \tilde{\omega}_i.$$

It is possible to compute $c_{i,j}$, Λ and \mathfrak{D} and to evaluate α at given points to high precision due to work of Paul Van Wamelen implemented in **MAGMA** [BCP97].

Proposition 26. *For each disk $V \in \mathcal{V}$, we can find an explicit compact box $\alpha[V]$ in \mathfrak{D} which contains the image $\alpha(V)$ of V under α , such that the diameters of such boxes tend to zero as $\rho \rightarrow 0$ uniformly in V .*

Write $\tilde{\rho}$ for such a uniform bound on the diameters.

Proof. Since the α_i are given by known linear combinations of the $\tilde{\alpha}_i$, it suffices to show this result for the $\tilde{\alpha}_i$. Let p_0 be the centre of V , and ρ the radius of its projection to $\mathbb{P}^1(\mathbb{C})$. Without loss of generality, we assume $|x_{p_0}| \leq |s_{p_0}|$. Throughout this proof, given $X \in \mathbb{C}$, $Y(X)$ will denote a square-root of $f(X)$, chosen to be continuous along radial paths if p_0 is a Weierstrass point, and otherwise chosen to have no branch cuts in V (the cover \mathcal{V} was carefully constructed so that this is possible).

Case 1: p_0 not a Weierstrass point

Fix $p \in V$. We parametrise the path $\gamma = \gamma_{p_0,p}$ by $X(\gamma(t)) = X_{p_0} + (X_p - X_{p_0})t$. Thus for all $i \in \{0, \dots, g-1\}$ we have

$$(77) \quad \begin{aligned} |\alpha_i(p_0) - \alpha_i(p)| &\leq \left| \int_{\gamma_{p_0,p}} \frac{X^i}{Y(X)} dX \right| \\ &\leq \int_{\gamma_{p_0,p}} \left| \frac{X^i}{Y(X)} \right| dX \\ &\leq \int_0^1 \left| \frac{X(\gamma(t))^i}{Y(X(\gamma(t)))} \right| |\gamma'(t)| dt \\ &\leq \rho \sup_{r \in B_\rho(X_{p_0})} \frac{|r|^i}{|\sqrt{f(r)}|} \end{aligned}$$

Case 2: p_0 is a Weierstrass point

Fix $p \in V$. We parametrise the path $\gamma = \gamma_{p_0,p}$ by $X(\gamma(t)) = X_{p_0} + (X_p -$

$X_{p_0})t^{3/2}$. Thus for all $i \in \{0, \dots, g-1\}$ we have

$$\begin{aligned}
 |\alpha(p_0)_i - \alpha(p)_i| &\leq \left| \int_{\gamma_{p_0, p}} \frac{X^i}{Y(X)} dX \right| \\
 (78) \quad &< \frac{3}{2} |X_{p_0} - X_p| \left| \int_0^1 \frac{X(\gamma(t))^i}{Y(X(\gamma(t)))} t^{1/2} dt \right| \\
 &\leq \frac{3}{2} \rho \sup_{r \in B_\rho(X_{p_0})} \frac{|r|^i}{\left| \sqrt{f(r)/(r - p_0)} \right|}
 \end{aligned}$$

It is easy to check that the given bounds tend to zero uniformly with ρ , so we are done. \square

10.4.2. *Bounds on the derivatives of theta functions.* To complete the proof of Case 1 of Proposition 25, we need the following lemma on the derivative of theta functions:

Lemma 27. *Fix $\epsilon > 0$. Let $z, w \in \mathbb{C}^g$ such that z lies within distance ϵ of the fundamental domain \mathfrak{D} , and w lies within distance ϵ of z (both distances in the L^1 metric). Let c_1 and c_2 be positive constants such that*

$$(79) \quad \max_i |\Im(z_i)| < \frac{c_1}{2\pi}, \quad \text{and} \quad \Im(\Lambda) \geq c_2.$$

Set $t(n) = \sqrt{\pi c_2}(n - \frac{c_1}{2\pi c_2})$, and write

$$A = \exp\left(\frac{c_1^2}{4\pi c_2}\right) \left(\sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} e^{-t(n)^2} + \frac{1}{2\sqrt{c_2}} \right),$$

and

$$B = 2\pi e^{\frac{c_1^2}{4\pi c_2}} \left(\frac{1}{\sqrt{\pi c_2}} \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil + 1} t(n) e^{-t(n)^2} + \frac{1}{2\sqrt{c_2}\pi} + \frac{c_1}{2\pi c_2} \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} e^{-t(n)^2} + \frac{c_1}{4\pi c_2^{3/2}} \right),$$

two constants independent of ϵ . Then we have the following bounds:

$$\begin{aligned}
 1) \quad & \left| \frac{\partial \vartheta}{\partial z_i}(z) \right| \leq 2^g A^{g-1} B \\
 2) \quad & |\vartheta(z) - \vartheta(w)| \leq \epsilon 2^g A^{g-1} B.
 \end{aligned}$$

Suppose also that $|\vartheta(z)| \geq c > 2^g A^{g-1} B$. Then

$$\begin{aligned}
 3) \quad & \left| \frac{\partial(1/\vartheta)}{\partial z_i}(z) \right| \leq (c - \epsilon 2^g A^{g-1} B)^{-2} 2^g A^{g-1} B \\
 4) \quad & \left| \frac{1}{\vartheta(z)} - \frac{1}{\vartheta(w)} \right| \leq \epsilon (c - \epsilon 2^g A^{g-1} B)^{-2} 2^g A^{g-1} B.
 \end{aligned}$$

Proof. Detailed background material for this proof may be found in [Mum83, II §1]. From the power series expansion

$$(80) \quad \vartheta(z) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^t \Lambda n + 2\pi i n \cdot z),$$

(here ι denotes a square-root of -1 , to distinguish it from the index i) we see

$$\begin{aligned}
\left| \frac{\partial^r \vartheta}{\partial z_j^r}(z) \right| &= \left| \sum_{n \in \mathbb{Z}^g} (\exp(\pi \iota n^t \Lambda n + 2\pi \iota n \cdot z) (2\pi \iota n_j)^r) \right| \\
&\leq \sum_{n \in \mathbb{Z}^g} \left(\exp \left(-\pi c_2 \sum_i n_i^2 + c_1 \sum_i |n_i| \right) (2\pi n_j)^r \right) \\
&\leq 2^g \sum_{n \in \mathbb{N}^g} \left(\exp \left(-\pi c_2 \sum_i n_i^2 + c_1 \sum_i n_i \right) (2\pi n_j)^r \right) \\
&\leq 2^g \left(\sum_{n \in \mathbb{N}} \exp(-\pi c_2 n^2 + c_1 n) \right)^{g-1} \left(\sum_{n \in \mathbb{N}} (2\pi n)^r \exp(-\pi c_2 n^2 + c_1 n) \right).
\end{aligned}$$

Now

$$(81) \quad \int_0^\infty x^r e^{-x^2} dx = \frac{1}{2} \Gamma \left(\frac{1+r}{2} \right),$$

so recalling $t(n) = \sqrt{\pi c_2} (n - \frac{c_1}{2\pi c_2})$, we obtain

$$\begin{aligned}
&\sum_{n \in \mathbb{N}} \exp(-\pi c_2 n^2 + c_1 n) \\
&= \exp \left(\frac{c_1^2}{4\pi c_2} \right) \sum_{n \in \mathbb{N}} \exp(-t(n)^2) \\
&\leq \exp \left(\frac{c_1^2}{4\pi c_2} \right) \left(\sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} \exp(-t(n)^2) + \int_{n=\lceil \frac{c_1}{2\pi c_2} \rceil}^\infty \exp(-t(n)^2) dn \right) \\
&\leq \exp \left(\frac{c_1^2}{4\pi c_2} \right) \left(\sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} \exp(-t(n)^2) + \frac{1}{\sqrt{\pi c_2}} \int_{t=0}^\infty \exp(-t^2) dt \right) \\
&= \exp \left(\frac{c_1^2}{4\pi c_2} \right) \left(\sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} \exp(-t(n)^2) + \frac{1}{2\sqrt{c_2}} \right).
\end{aligned}$$

Now we must do the same for $\sum_{n \in \mathbb{N}} (2\pi n) \exp(-\pi c_2 n^2 + c_1 n)$ (exactly the same argument would work for the r th derivative, but we need only the first derivative):

$$\begin{aligned}
&\sum_{n \in \mathbb{N}} (2\pi n) \exp(-\pi c_2 n^2 + c_1 n) = 2\pi \exp \left(\frac{c_1^2}{4\pi c_2} \right) \sum_{n \in \mathbb{N}} n \exp(-t(n)^2) \\
&= 2\pi \exp \left(\frac{c_1^2}{4\pi c_2} \right) \left(\frac{1}{\sqrt{\pi c_2}} \sum_{n \in \mathbb{N}} t(n) \exp(-t(n)^2) + \frac{c_1}{2\pi c_2} \sum_{n \in \mathbb{N}} \exp(-t(n)^2) \right).
\end{aligned}$$

Now

(82)

$$\begin{aligned}
\sum_{n \in \mathbb{N}} t(n) \exp(-t(n)^2) &\leq \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil + 1} t(n) \exp(-t(n)^2) + \int_{n=\lceil \frac{c_1}{2\pi c_2} \rceil}^{\infty} |t(n)| \exp(-t(n)^2) \, dn \\
&\leq \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil + 1} t(n) \exp(-t(n)^2) + \frac{1}{\sqrt{\pi c_2}} \int_{t=0}^{\infty} t \exp(-t^2) \, dt \\
&= \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil + 1} t(n) \exp(-t(n)^2) + \frac{1}{2\sqrt{\pi c_2}},
\end{aligned}$$

so combining the above results we find

$$\begin{aligned}
&\sum_{n \in \mathbb{N}} (2\pi n) \exp(-\pi c_2 n^2 + c_1 n) \leq \\
&2\pi \exp\left(\frac{c_1^2}{4\pi c_2}\right) \left(\frac{1}{\sqrt{\pi c_2}} \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil + 1} t(n) e^{-t(n)^2} + \frac{1}{2\sqrt{c_2 \pi}} + \frac{c_1}{2\pi c_2} \sum_{n=0}^{\lceil \frac{c_1}{2\pi c_2} \rceil} e^{-t(n)^2} + \frac{c_1}{4\pi c_2^{3/2}} \right).
\end{aligned}$$

This concludes the computation of the bounds for (1). The bound for (2) is simple; it is simply ϵ times the bound for (1). For (3), we use

$$(83) \quad \frac{\partial(1/\vartheta)}{\partial z_i}(z) = \frac{-1}{\vartheta(z)^2} \frac{\partial \vartheta}{\partial z_i}(z)$$

to conclude that the bound for (3) is $(c - \epsilon 2^g A^{g-1} B)^{-2}$ times the bound for (1), and similarly that the bound for (4) is ϵ times the bound for (3). \square

10.5. Case 2: p_0 and q_0 both Weierstrass points. In this case, both the numerator and denominator of (71) vanish to order $g(g-1)/2$ at p_0 . To approximate the value of the expression at (p_0, q_0) is not hard using a limiting approach, but to control the derivative near to that point would be more difficult. Instead, we apply the maximum modulus principle and take advantage of the symmetry of the situation to reduce to Case 1.

As before, write V_{p_0} and V_{q_0} for the non-overlapping disks centered at p_0 and q_0 in \mathcal{V} . Using the maps induced in Section 9.2.2, we shall abuse notation by viewing V_{p_0} and V_{q_0} as open discs in \mathbb{C} . Recall that $\alpha : C \rightarrow \mathfrak{D}$ is the map to a fundamental domain inside \mathbb{C}^g obtained by integrating. Then write

$$(84) \quad \begin{aligned} \phi : V_{p_0} \times V_{q_0} &\rightarrow \mathbb{C} \\ (p, q) &\mapsto \frac{\vartheta(g\alpha(p) - \alpha(q))}{\prod_{w \in W} \vartheta(g\alpha(p) - w)}, \end{aligned}$$

and

(85)

$$K(p, q) = S(X) \det(\Im(\tau)^{1+g-g^3}) \frac{\exp(-\pi \Im(g\alpha(p) - \alpha(q))^t (\Im(\tau))^{-1} \Im(g\alpha(p) - \alpha(q)))}{\prod_{w \in W} \exp(-\pi \Im(g\alpha(p) - \alpha(w))^t (\Im(\tau))^{-1} \Im(g\alpha(p) - \alpha(w)))},$$

where the product is over Weierstrass points w counted with their weights (which we recall are all $g(g-1)/2$ in the hyperelliptic case).

Then ϕ is related to the g th power of the Green's function by

$$(86) \quad G(p, q)^g = |\phi(p, q)| K(p, q),$$

and so to bound

$$(87) \quad G(p, q)^g,$$

it suffices to bound $|\phi(p, q)|$ and $K(p, q)$ separately.

Bounding $K(p, q)$ is straightforward; Since $\Im(\tau)$ is positive definite, $\Im(\tau)^{-1}$ is also, and so it is sufficient to ensure that the values of $g\alpha(p) - \alpha(q)$ and $g\alpha(p) - \alpha(w)$ do not get too small. This is achieved by making a suitable choice of fundamental domain \mathfrak{D} .

To bound $\phi(p, q)$ on $V_{p_0} \times V_{q_0}$ is a little harder, since it is written as a quotient of two holomorphic functions which both vanish to the same degree; bounding the numerator and denominator separately will not be sufficient. Instead, we will apply the maximum modulus principle, using the following lemma:

Lemma 28. *Retaining the setup above, there exists a computable union of eight subsets $\mathbb{V}_i \subset C \times C$ with the following properties:*

- 1) $\sup_{(p,q) \in V_{p_0} \times V_{q_0}} |\phi(p, q)| \leq \max_{i \in \{1, \dots, 8\}} \sup_{(p,q) \in \mathbb{V}_i} \phi(p - q)$.
- 2) *For each i , at least one of p and q is never a Weierstrass point for $(p, q) \in \mathbb{V}_i$.*

Proof. The construction of the \mathbb{V}_i is simple; they are the eight 3-real-dimensional faces of a 4-real-dimensional cube contained in $C \times C$, centered at (p_0, q_0) and chosen just large enough to contain $V_{p_0} \times V_{q_0}$. It is easy but un-illuminating to write down parametrisations of the faces.

Assertion (1) now follows immediately from the maximum modulus principle applied to this cube.

It is easy to check that this closed cube does not contain any images of Weierstrass points apart from p_0 and q_0 , and on each face at least one of the real or imaginary parts of either p or q is constrained to be unequal to the corresponding coordinate of p_0 or q_0 respectively, so (2) follows also. \square

Using this lemma, we see that we may apply the derivative bounds from Lemma 27 to enable us to numerically bound the supremum of $|\phi(p, q)|$ for $(p, q) \in \mathbb{V}_i$; on a fixed \mathbb{V}_i , we know from (2) that at least one of p or q is never a Weierstrass point, so (possibly after interchanging p and q), the expression for ϕ is given as a ratio of *non-vanishing* holomorphic functions, whose derivatives are bounded in Lemma 27, and which we may therefore rigorously numerically bound.

This gives us an upper bound on $|\phi(p, q)|$ for $(p, q) \in V_{p_0} \times V_{q_0}$. We also need a positive lower bound, but this is easily obtained by applying the same algorithm to the function $1/\phi(p, q)$.

11. THE FIRST NAÏVE HEIGHT

Recall that $K = \mathbb{Q}$.

Definition 29. We begin by defining a naïve height $\tilde{H} : A(K) \rightarrow \mathbb{R}_{>1}$. Note that it does not arise directly from a projective embedding, but we still call it ‘naïve’ since it is relatively simple to define and compute, and is an approximation of the Néron-Tate height (as we will shortly prove).

Let $\mu > 0$ be less than half of the shortest distance between any two Weierstrass points under the Archimedean absolute value of K .

Given $p \in A(K)$, write $p = [D - \deg(D)\infty]$ where D is a reduced divisor on C . If the support of D contains any Weierstrass points, replace D by the divisor obtained by subtracting them off; this equates to translating p by a 2-torsion point, and so will not affect the Néron-Tate height. Let d denote the degree of the resulting divisor D .

Choose once and for all a pair of degree- d effective divisors ∞_p^1 and ∞_p^2 with disjoint support, supported on Weierstrass points away from ∞ , such that no point in the support of D is within Archimedean distance μ of any point in the support of ∞_p^1 or ∞_p^2 . The existence of such divisors is clear since there are $2g + 1$ Weierstrass points away from ∞ and reduced divisors have degree g .

Recalling that D^- denotes the image of D under the hyperelliptic involution, define

$$(88) \quad \tilde{H}(p) = \left(\prod_{\nu \in M_L} \frac{1}{d_\nu(D - \infty_p^1, D^- - \infty_p^2)} \right)^{\frac{1}{[L:K]}},$$

where L/K is the minimal finite extension over which D , ∞_p^1 and ∞_p^2 are pointwise rational, recalling that if $D = \sum_i d_i$, $\infty_p^1 = \sum_i q_i^1$ and $\infty_p^2 = \sum_i q_i^2$ then

$$(89) \quad d_\nu(D - \infty_p^1, D^- - \infty_p^2) = \prod_{i,j} \frac{d_\nu(p_i, p_j^-) d_\nu(q_i^1, q_j^2)}{d_\nu(p_i, q_i^2) d_\nu(p_i^-, q_i^1)}.$$

We define a logarithmic naïve height by $\mathcal{H}(p) = \log(\tilde{H}(p))$.

Remark 30. Note that in the above definition, we made use of the assumption that $K = \mathbb{Q}$ - indeed, this is the only point at which we use this fact. The condition would not be hard to remove by allowing different choices of divisors ∞_p^1 and ∞_p^2 at different Archimedean absolute values, and then showing that the change to the resulting height was not too large.

Proposition 31. The products in the definition above are finite; in particular, the heights are well defined.

Proof. From the definitions of the metrics over non-Archimedean absolute values, it is clear that $d_\nu(D - \infty_p^1, D^- - \infty_p^2) = 1$ for all but finitely many such absolute values. \square

Combining previous results, we obtain the following theorem, which is the main result of this paper.

Theorem 32. For all $p \in A(K)$ we have

$$(90) \quad \left| \hat{h}(p) - \mathcal{H}(p) \right| \leq \mathcal{B}_1 + \mathcal{B}_2 + \mathcal{B}_3,$$

where \mathcal{B}_1 is from Definition 7, \mathcal{B}_2 is from Corollary 8 and \mathcal{B}_3 is from Definition 21.

Write c for the constant $\mathcal{B}_1 + \mathcal{B}_2 + \mathcal{B}_3$.

12. REFINED NAÏVE HEIGHTS

We define two new naïve heights which are each in turn simpler to compute, and we bound their difference from the Nèron-Tate height. The last of these heights will be sufficiently simple as to allow us to give an algorithm to solve the saturation problem.

Definition 33. Given $p \in A(K)$, we take the divisor $D = \sum_{i=1}^d p_i$ over some finite L/K as in Definition 29, and write $p_i = (X_i, Y_i)$. Then set

$$(91) \quad h^\heartsuit(p) = \sum_{i=1}^d h(X_{p_i}),$$

and set

$$(92) \quad h^\dagger(p) = h\left(\prod_{i=1}^d (X - X_{p_i})\right),$$

where the right hand side is the height of a polynomial, which equals the height of the point in projective space whose coordinates are given by its coefficients. Given $B > 0$, define

$$(93) \quad M^\heartsuit(B) = \{p \in A(K) : h^\heartsuit(p) \leq B\}$$

and

$$(94) \quad M^\dagger(B) = \{p \in A(K) : h^\dagger(p) \leq B\}$$

Our main aim in this section is to give computable bounds on the differences $|\mathcal{H} - h^\heartsuit|$ and $|h^\heartsuit - h^\dagger|$.

Lemma 34. There exist computable constants $0 < c_1 < c_2$ with the following property:

for all non-Weierstrass points $p = (x : s : y) \in C(K)$, and for all Archimedean norms $|\cdot|_\nu$ on K , we have

$$(95) \quad c_1 \leq d_\nu(p, p^-) / (2 \min(|Y|_\nu, |Y'|_\nu)) \leq c_2,$$

where as usual we write $Y = y/s^{g+1}$ and $Y' = y/x^{g+1}$.

Proof. Fix an Archimedean absolute value ν . Recall that $d = d_\nu$ is the weak-pseudo-metric given in Definition 18 using a Merkl atlas. There are two cases to consider.

Case 1: there is no chart U in the Merkl atlas such that $p \in U^{r_1}$ and $p^- \in U^{r_1}$. Then the value of $d(p, p^-)$ must be one of a finite set of positive values (as defined in 18). We also note that $\min(|Y|_\nu, |Y'|_\nu)$ is bounded above (for obvious reasons) and is also bounded below since p cannot be too close to a Weierstrass point (otherwise p and p^- would both be contained in the same Merkl chart), and so $\min(|Y|_\nu, |Y'|_\nu)$ is bounded away from zero, to the result follows.

Case 2: there is a Merkl chart U with $p \in U^{r_1}$ and $p^- \in U^{r_1}$. Clearly such a chart must contain (and so be centred at) a Weierstrass point, call it

$w = (x_w : s_w : y_w)$. Without loss of generality say $|x_w|/|e|s_w|$, so there is a $t > 1$ such that $|x_p/s_p| \leq t$. Then $|Y| \leq |Y'|t^g$, so it suffices to show that $|Y|$ is close to $d(p, p^-)$. Now $d(p, p^-)$ is given by the following procedure:

Translate w to the point $X = 0$ using a Möbius transformation by an orthogonal matrix

$$(96) \quad M = \begin{pmatrix} 1 & -X_w \\ -\overline{X_w} & -1 \end{pmatrix}$$

Then $d(p, p^-) = 2 \left| \sqrt{X(p)} \right|$. Thus

$$(97) \quad d(p, p^-) = 2 \left| \sqrt{\frac{X_p - X_w}{X_p \overline{X_w} + 1}} \right|,$$

whereas

$$(98) \quad 2|Y_p| = 2 \left| \sqrt{(X_p - X_w) \cdot f_w} \right|,$$

where $f_w(t) = f(t)/(t - X_w)$. Thus by bounding the rational function

$$(99) \quad (X - X_w)/f_w$$

on the domain (recalling that R is the constant defined in 4.2.1)

$$(100) \quad \{X \in \mathbb{C} : |M \cdot X| \leq R\}$$

(a region on which, by construction, it has neither zeros nor poles), we are done. \square

Definition 35. Let L/K be a finite extension, and let $p \neq q \in C(L)$ be distinct points. Set

$$(101) \quad \langle p, q \rangle_L = \frac{-1}{[L : K]} \log \prod_{\nu \in M_L} d_\nu(p, q).$$

Lemma 36. There exists a computable constant c with the following property:

let L/K be a finite extension, and let $p = (x : s : y) \in C(L)$ be a non-Weierstrass point. Then

$$(102) \quad |\langle p, p^- \rangle_L - (g+1)h(x/s)| \leq c$$

Proof. For $|\cdot|$ non-Archimedean, we have that if $|x| \leq |s|$ then $d(p, p^-) = |2y/s^{g+1}|$, and if $|s| \leq |x|$ then $d(p, p^-) = |2y/x^{g+1}|$. Hence for non-Archimedean ν we obtain

$$(103) \quad d_\nu(p, p^-) = |2y|_\nu \min(1/|x|_\nu^{g+1}, 1/|s|_\nu^{g+1}).$$

We have shown above that for Archimedean ν we have computable $0 < c_1 < c_2$ such that

$$(104) \quad c_1 < d_\nu(p, p^-) / \min(|2y/x^{g+1}|, |2y/s^{g+1}|) < c_2.$$

Hence

$$(105) \quad \prod_{\nu \in M_L^\infty} 1/c_2 \leq \frac{\prod_{\nu \in M_L} 1/d_\nu(p, p^-)}{\prod_{\nu \in M_L} |2y|_\nu^{-1} \prod_{\nu \in M_L} \max(|x|_\nu, |s|_\nu)^{g+1}} \leq \prod_{\nu \in M_L^\infty} 1/c_1.$$

Now $\prod_{\nu \in M_L^\infty} c_1^{-1/[L:K]}$ is bounded uniformly in L , and similarly for c_2 . Finally, note

$$(106) \quad \left(\prod_{\nu \in M_L} |2y|_\nu^{-1} \right) \left(\prod_{\nu \in M_L} \max(|x|_\nu, |s|_\nu) \right)^{g+1} = H(x/s)^{[L:K](g+1)}.$$

□

Definition 37. Assume that the hyperelliptic polynomial f is monic. Given a Weierstrass point d with $s_d \neq 0$, set \tilde{f}_d to be the univariate polynomial such that for all $p \neq d \in C(K)$, we have

$$(107) \quad \tilde{f}_d(X_p)(X_p - X_d) = f(X_p).$$

It is clear that \tilde{f}_d will have integral coefficients, since f does and X_d is a root of f .

Lemma 38. Let L/K be a finite extension, and let $p, d \in C(L)$ such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Assume further that the hyperelliptic polynomial f is monic, so that X_d is integral. Let ν be a non-Archimedean absolute value of L , and suppose $|X_p - X_d|_\nu < \left| \tilde{f}_d(X_d) \right|_\nu$. Then

$$(108) \quad |Y_p|_\nu^2 = |X_p - X_d|_\nu \left| \tilde{f}_d(X_d) \right|_\nu.$$

Proof. By definition, we have

$$(109) \quad |Y_p|_\nu^2 = |X_p - X_d|_\nu \left| \tilde{f}_d(X_p) \right|_\nu,$$

so it suffices to show that $\left| \tilde{f}_d(X_p) \right|_\nu = \left| \tilde{f}_d(X_d) \right|_\nu$. Writing

$$(110) \quad \tilde{f}_d(X_p) = (X_p - X_d)^n + \star(X_p - X_d)^{n-1} + \cdots + \star(X_p - X_d) + \tilde{f}_d(X_d)$$

where the coefficients \star are integral, we see that the greatest norm of any term on the right hand side is achieved by $\tilde{f}_d(X_d)$ and no other term, so the result follows. □

Lemma 39. Let L/K be a finite extension, and let $p \neq d \in C(L)$ be such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Assume further that the hyperelliptic equation f is monic, so that X_d is integral. Then

$$(111) \quad - \sum_{\nu \in M_L^0} \log d_\nu(p, d) \leq [L : K] \left(\frac{1}{2} h(X_p - X_d) + h(\tilde{f}_d(X_d)) \right).$$

Note that the sum is over the non-Archimedean absolute values.

Proof. The right hand side naturally decomposes as

$$(112) \quad [L : K] \left(\frac{1}{2} h(X_p - X_d) + h(\tilde{f}_d(X_d)) \right) = \sum_{\nu \in M_L} \frac{1}{2} \log^+ |X_p - X_d|_\nu^{-1} + \log^+ \left| \tilde{f}_d(X_d) \right|_\nu^{-1}.$$

Now it is clear that

$$(113) \quad \sum_{\nu \in M_L^\infty} \frac{1}{2} \log^+ |X_p - X_d|_\nu^{-1} + \log^+ \left| \tilde{f}_d(X_d) \right|_\nu^{-1} \geq 0,$$

so it suffices to prove that for each non-Archimedean ν we have

$$(114) \quad -\log(d_\nu(p, d)) \leq \frac{1}{2} \log^+ |X_p - X_d|_\nu^{-1} + \log^+ \left| \tilde{f}_d(X_d) \right|_\nu^{-1},$$

or equivalently that (at this point we drop the subscript ν from the norm)

$$(115) \quad d_\nu(p, d)^{-2} \leq \max(|X_p - X_d|^{-1}, 1) \max\left(\left| \tilde{f}_d(X_d) \right|^{-1}, 1\right)^2.$$

Recalling that $\left| \tilde{f}_d(X_d) \right| \leq 1$ and writing $F = \left| \tilde{f}_d(X_d) \right|$ for simplicity, we see this is equivalent to showing

$$(116) \quad d_\nu(p, d)^2 \geq F^2 \min(|X_p - X_d|, 1).$$

We divide proving this in to two cases. The first is when $|X_p - X_d| \geq F$. Then

$$(117) \quad d_\nu(p, d) \geq \begin{cases} F & \text{if } |X_p| \leq 1 \\ 1 & \text{if } |X_p| > 1, \end{cases}$$

so Equation (116) follows.

The harder case is when $|X_p - X_d| < F$. We apply Lemma 38 to see that $|Y_p|^2 = |X_p - X_d| F$, and so

$$(118) \quad \begin{aligned} d_\nu(p, d)^2 &= \begin{cases} \max(|X_p - X_d|^2, |Y_p|^2) & \text{if } |X_p| \leq 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\ &= \begin{cases} \max(|X_p - X_d|^2, |X_p - X_d| F) & \text{if } |X_p| \leq 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\ &\geq \begin{cases} F \max(|X_p - X_d|^2, |X_p - X_d|) & \text{if } |X_p| \leq 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\ &= \begin{cases} F |X_p - X_d| & \text{if } |X_p| \leq 1 \\ 1 & \text{if } |X_p| > 1 \end{cases} \\ &\geq F \min(|X_p - X_d|, 1) \\ &\geq F^2 \min(|X_p - X_d|, 1) \end{aligned}$$

□

Lemma 40. *Let $X_1, X_2 \in L$. Then*

$$(119) \quad H(X_1 + X_2) \leq 2^{\#M_L^\infty / [L:K]} H(X_1) H(X_2).$$

Proof.

$$(120) \quad \begin{aligned} H(X_1 + X_2)^{[L:K]} &= \prod_{\nu \in M_L} \max(1, |X_1 + X_2|_\nu) \\ &\leq \left(\prod_{\nu \in M_L^0} \max(1, |X_1|_\nu, |X_2|_\nu) \right) \left(\prod_{\nu \in M_L^\infty} \max(1, |X_1|_\nu + |X_2|_\nu) \right) \\ &\leq \left(\prod_{\nu \in M_L^0} \max(1, |X_1|_\nu) \max(1, |X_2|_\nu) \right) \left(\prod_{\nu \in M_L^\infty} 2 \max(1, |X_1|_\nu) \max(1, |X_2|_\nu) \right) \\ &= 2^{\#M_L^\infty} H(X_1)^{[L:K]} H(X_2)^{[L:K]} \end{aligned}$$

as required. \square

Lemma 41. *Fix $\mu > 0$ and $n \in \mathbb{N}$. There exists a computable constant $\phi_\mu(n)$ with the following property:*

Let L/K be a finite extension of degree at most n , and let $p, d \in C(L)$ such that $s_p \neq 0$ and d is a Weierstrass point with $s_d \neq 0$. Assume further that the hyperelliptic equation f is monic, and also that for all Archimedean absolute values $\nu \in M_L^\infty$, we have $d_\nu(p, d) \geq \mu$. Then

$$(121) \quad \langle p, d \rangle_L \leq \frac{1}{2} h(X_p) + \phi_\mu(n).$$

Proof. From Lemma 39 and the fact that $d_\nu(p, d) \geq \mu$ for all Archimedean ν , we see that

$$(122) \quad \langle p, d \rangle_L \leq \frac{1}{2} h(X_p - X_d) + h(\tilde{f}_d(X_d)) - \log(\mu) \# M_L^\infty / [L : K].$$

Now by Lemma 40, we have

$$(123) \quad h(X_p - X_d) \leq h(X_p) + h(X_d) + \frac{\# M_L^\infty}{[L : K]} \log(2),$$

so for fixed L and d we may take

$$(124) \quad \phi_\mu^{L,d}(n) = \frac{1}{2} h(\tilde{f}_d(X_d)) - \log(\mu) \frac{\# M_L^\infty}{[L : K]} + h(X_d) + \frac{\# M_L^\infty}{2[L : K]} \log(2).$$

Thus the existence of a bound uniform in L and d is clear (since there are only finitely many Weierstrass points, and the degree of L is bounded). \square

Lemma 42. *There exists a computable constant c such that the following holds:*

given $p \in A(K)$, let D, ∞_p^1 and ∞_p^2 denote the divisors given in Definition 29. Let L/K be the minimal finite extension such that D, ∞_p^1 and ∞_p^2 are all pointwise rational over L . Then we may write

$$(125) \quad \begin{aligned} D &= \sum_{i=1}^d p_i \\ \infty_p^1 &= \sum_{i=1}^d q_i \\ \infty_p^2 &= \sum_{i=1}^d q'_i. \end{aligned}$$

Then

$$(126) \quad \mathcal{H}(p) \geq \sum_{i=1}^d \left(\langle p_i, p_i^- \rangle_L - \sum_{j=1}^d \langle p_i, q_j \rangle_L - \sum_{j=1}^d \langle p_i, q'_j \rangle_L \right) + c.$$

Proof. Recall that

$$(127) \quad \mathcal{H}(p) = \sum_{i,j=1}^d \langle p_i, p_j^- \rangle_L + \sum_{i,j=1}^d \langle q_i, q'_j \rangle_L - \sum_{i,j=1}^d \langle p_i, q_j \rangle_L - \sum_{i,j=1}^d \langle p_i^-, q'_j \rangle_L.$$

Since the q_i and q'_i are distinct Weierstrass points we easily bound $\sum_{i,j=1}^d \langle q_i, q'_j \rangle_L$. For $i \neq j$, we have by Theorem 16 that

$$(128) \quad \langle p_i, p_j^- \rangle_L \geq -\mathcal{B}(\mathbb{M}) \cdot \#M_L^\infty/[L : K] - \mathcal{B}_1,$$

where \mathbb{M} is the Merkl atlas constructed in Section 9.2 (since all other contributions to the pairing are non-negative), so the result follows. \square

Lemma 43. *There exists a computable constant c' such that in the setup of Lemma 42 we have*

$$(129) \quad \mathcal{H}(p) \geq \sum_{i=1}^d h(X_{p_i}) + c'$$

Proof. In Lemma 42 we showed

$$(130) \quad \mathcal{H}(p) \geq \sum_{i=1}^d \left(\langle p_i, p_i^- \rangle_L - \sum_{j=1}^d \langle p_i, q_j \rangle_L - \sum_{j=1}^d \langle p_i, q'_j \rangle_L \right) + c.$$

In Lemma 36 we showed (using that the p_i are never Weierstrass points) that for some computable c_1 we have

$$(131) \quad |\langle p_i, p_i^- \rangle_L - (g+1)h(X_{p_i})| \leq c_1.$$

Write n for a positive integer such that the minimal field L appearing in Definition 29 can always be taken to have degree at most n (this n will depend only on the genus of the curve C). In Lemma 41 we showed (using that $d_\nu(p_i, q_j) \geq \mu$ where μ is as in Definition 29) that

$$(132) \quad \langle p_i, q_j \rangle_L \leq \frac{1}{2}h(X_{p_i}) + \phi_\mu(n),$$

and similarly for q'_j .

Combining these, we see using $d \leq g$ that for each i

$$(133) \quad \begin{aligned} \langle p_i, p_i^- \rangle_L - \sum_{j=1}^d \langle p_i, q_j \rangle_L - \sum_{j=1}^d \langle p_i, q'_j \rangle_L &\geq (g+1)h(X_{p_i}) - 2 \sum_{j=1}^d \frac{1}{2}h(X_{p_i}) - c_1 + 2d\phi_\mu(n) \\ &= ((g+1) - 2d\frac{1}{2})h(X_{p_i}) - c_1 + 2d\phi_\mu(n) \\ &\geq h(X_{p_i}) - c_1 + 2d\phi_\mu(n). \end{aligned}$$

from which the result follows. \square

Theorem 44. *There exists a computable constant c such that for all $p \in A(K)$ we have*

$$(134) \quad \hat{h}(p) + c \geq h^\heartsuit(p).$$

Proof. From Theorem 32 we know that there exists a computable constant c' such that

$$(135) \quad \hat{h}(p) + c' \geq \mathcal{H}(p).$$

The result follows from combining this with Lemma 43. \square

Corollary 45. *For any constant B :*

$$(136) \quad \hat{M}(B) \subset M^\heartsuit(B + c)$$

where c is the computable constant from Theorem 44.

Lemma 46. *Fix a finite extension L/K . Given $a_1, \dots, a_n \in L$, set $\psi_n = \prod_{i=1}^n (t - a_i)$. Then*

$$(137) \quad \left| h(\psi_n) - \sum_{i=1}^n h(a_i) \right| \leq \#M_K^\infty \log(4)(n^2 + n - 2)/2.$$

Proof. From [Lan83, Chapter 3, Proposition 2.4] we have for all $m \geq 2$ that

$$(138) \quad |h(t - a_m) + h(\psi_{m-1}) - h(\psi_m)| \leq m \#M_K^\infty \log(4)$$

(note the difference in normalisations between our heights and Lang's). The formula follows by induction and using that $h(t - a_i) = h(a_i)$. \square

Corollary 47. *For all $p \in A(K)$ we have*

$$(139) \quad \left| h^\heartsuit(p) - h^\dagger(p) \right| \leq \#M_K^\infty \log(4)(g^2 + g - 2)/2.$$

The main result of this chapter is then

Theorem 48. *Let c be the computable constant from Theorem 44. Then for all constants B we have*

$$(140) \quad \hat{M}(B) \subset M^\dagger(B + c + \#M_K^\infty \log(4)(g^2 + g - 2)/2).$$

The point is that these finite sets $M^\dagger(B)$ are effectively computable, so we can in turn use the results from [Hol12a] to compute the finite sets $\hat{M}(B)$. We describe one algorithm to compute $M^\dagger(B)$, setting $K = \mathbb{Q}$ for simplicity:

1) Let S be the finite set of all polynomials $\prod_{i=1}^d (X - a_i)$, for $d \leq g$, of height up to B .

2) for each polynomial $a \in S$, if a is not irreducible remove it from S and insert into S each of the irreducible factors of a .

3) it suffices to determine for each $a \in S$ whether a is the ‘ x -coordinate polynomial’ of a divisor in Mumford representation; in other words, whether there exists another univariate polynomial b such that (a, b) satisfy the properties of a Mumford representation. Now the polynomial a also determines a set of $2 \deg(a)$ distinct complex points on C - the preimages of zeros of a under the hyperelliptic projection. These can be computed to any finite precision. Such points will satisfy $y = b(x)$, thus if we can bound the denominators of the coefficients of b then we can find a finite precision to which we need to compute the complex points to see if they correspond to a polynomial b with rational coefficients. Such a bound on the denominators is supplied by the following proposition.

Proposition 49. *Let K/\mathbb{Q} be a finite extension, with integers \mathcal{O}_K and p a prime ideal in \mathcal{O}_K . Let $g > 0$ be an integer. Let $f, h \in K[x]$ be polynomials which are integral with respect to p (ie the p -adic valuation of their coefficients are positive) and such that*

- $4f + h^2$ is separable;
- f has degree $2g + 1$;

- h has degree at most $g + 1$.

Fix an integer $1 \leq d \leq g$. Suppose we are given a pair of polynomials $a = \sum_{i=0}^d a_i x^i$ of degree d and $b = \sum_{i=0}^{d-1} b_i x^i$ of degree at most $d-1$ in $K[x]$ and a constant $c \in K$ with the following properties:

- a, b and c are integral at p (ie their p -adic valuations are positive);
- a is primitive;
- $\text{ord}_p c > \min_i (\text{ord}_p b_i)$;
- $\Delta = \text{disc}(a)$ is non-zero.

Suppose also that

$$(141) \quad a \mid \left(\frac{b}{c}\right)^2 + \left(\frac{b}{c}\right) \cdot h - f.$$

Then

$$(142) \quad \text{ord}_p c \leq \frac{1}{2} \text{ord}_p \Delta + \left(d^2 - d + \max\left(\frac{2g+1}{2}, \deg(h)\right)\right) \text{ord}_p a_d.$$

Proof. Let L be a ‘sufficiently large’ extension of the completion K_p ; by this we mean that L is a finite extension of the completion which we will require to be closed under taking roots of a certain finite collection of polynomials, which will be described as we go along. Let π denote a uniformiser of L , and \mathcal{O}_L its integers.

We assume a splits in L ; write x_1, \dots, x_d for the roots. Each x_i may be uniquely written as $x_i = \tilde{x}_i / \pi^{r_i}$ where $r_i \geq 0$ and $\tilde{x}_i \in \mathcal{O}_L$ has minimal valuation. Let

$$(143) \quad \tilde{a} = \prod_{i=1}^d (\pi^{r_i} x - \tilde{x}_i) \in \mathcal{O}_L[x].$$

Now a and \tilde{a} have the same degree and (distinct) roots, are integral, and both have at least one coefficient which is a unit in \mathcal{O}_L , hence a and \tilde{a} differ by a unit in \mathcal{O}_L .

Let

$$(144) \quad \widetilde{M} = \begin{pmatrix} \pi^{(d-1)r_1} & \pi^{(d-2)r_1} \tilde{x}_1 & \dots & \tilde{x}_1^{d-1} \\ \pi^{(d-1)r_2} & \pi^{(d-2)r_2} \tilde{x}_2 & \dots & \tilde{x}_2^{d-1} \\ \vdots & & & \\ \pi^{(d-1)r_d} & \pi^{(d-2)r_d} \tilde{x}_d & \dots & \tilde{x}_d^{d-1} \end{pmatrix},$$

so $\det(\widetilde{M})^2 = \text{disc}(\tilde{a}) = \text{unit} \times \Delta$. Let

$$(145) \quad M = \begin{pmatrix} 1 & x_1 & \dots & x_1^{d-1} \\ 1 & x_2 & \dots & x_2^{d-1} \\ \vdots & & & \\ 1 & x_d & \dots & x_d^{d-1} \end{pmatrix}.$$

By (141) we know that for all $1 \leq i \leq d$ we have

$$(146) \quad \sum_{j=0}^{d-1} \left(\frac{b_j}{c}\right) x_i^j = y_i$$

for some y_i in L (obtained by assuming L sufficiently large) satisfying $y_i^2 + h(x_i)y_i = f(x_i)$, and hence that

$$(147) \quad \frac{1}{c} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{d-1} \end{pmatrix} = M^{-1} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_d \end{pmatrix}.$$

In order to bound above the order of c at π , it therefore suffices to bound below the order of the right hand side of (147) at π . We do this in two steps. Firstly, we easily obtain from properties of valuations that

$$(148) \quad \text{ord}_\pi y_i \geq -r_i \max \left(\frac{2g+1}{2}, \deg(h) \right).$$

Secondly, we must do the same for M^{-1} . Now $M \cdot \pi^{(d-1)\max_i r_i}$ is a matrix over \mathcal{O}_L , and hence so is its transposed matrix of cofactors, which we shall denote M_c . We then find that

$$(149) \quad M^{-1} = \frac{1}{\pi^{d(d-1)\max_i r_i}} \times \frac{1}{\det(M)} \times M_c.$$

We also compute that

$$(150) \quad \begin{aligned} \det(M) &= \pi^{-(d-1)\sum_i r_i} \det(\widetilde{M}) \\ &= \pi^{-(d-1)\sum_i r_i} \sqrt{\Delta \cdot \text{unit}}, \end{aligned}$$

and hence

$$(151) \quad M^{-1} = \frac{M_c}{\sqrt{\Delta \cdot \text{unit}} \pi^{d(d-1)\max_i(r_i) - (d-1)\sum_i r_i}}.$$

We also note that $\sum_i r_i = \text{ord}_\pi a_d$, and $\max_i(r_i) \leq \sum_i r_i$, so combining the above results we see that

$$(152) \quad \text{ord}_\pi c \leq \frac{1}{2} \text{ord}_\pi \Delta + \left((d-1)^2 + \max \left(\frac{2g+1}{2}, \deg(h) \right) \right) \text{ord}_\pi a_d,$$

from which the result immediately follows. \square

We note that in the elliptic case, we recover the classical result that $c^2 \mid a_1^3$.

13. APPENDIX: AN ALGORITHM TO COMPUTE A COVER OF THE RIEMANN SPHERE

In this appendix, we will describe an algorithm to determine a cover of the Riemann sphere by open discs in the chordal metric, satisfying certain technical hypotheses coming from Merkl's theorem.

Let S^2 denote the Riemann sphere, and fix $r < 1$. By an 'algebraic point of S^2 ' we mean a point which maps to an element of \mathbb{Q}^{alg} in \mathbb{C} . Note that such a point can be described by a finite amount of data.

Definition 50. *We say a closed subset $Z \subset S^2$ is 'starry' if the complement of Z is a finite union of open discs (in the chordal metric) of radius $r < 1$ centred at algebraic points.*

Proposition 51. *Suppose Z is starry, has no isolated points and the interior Z° is non-empty. Then there exists an algorithm to find an algebraic point $p \in Z^\circ$ such that $Z \setminus B_r(p)$ has no isolated points.*

Proof. The set of points p such that $Z \setminus B_r(p)$ has isolated points is contained in the set of points p such that there exist q_1, q_2 centres of discs in the complement Z^c and $t \in Z$ with

$$(153) \quad d(p, t) = d(t, q_1) = d(t, q_2) = r.$$

The set of such points p is contained in a finite union of computable circles (boundaries of discs) of radius r and centred at algebraic points, and so the complement of that set in Z° is non-empty open and described by a finite collection of computable conditions, and we can find an algebraic point inside it. \square

Proposition 52. *Let Z be starry. Then every connected component of Z has either non-empty interior, or is an isolated point.*

Proof. Fix a connected component Y . If $Y^\circ = \emptyset$, then $Y = \partial Y$, so Y is a finite union of circles of radius r . Since the complement of Z can be covered by a finite collection of open discs D_i of radius r , we see that there must be a segment of Y of positive length which is touched by exactly two of the D_i . These discs therefore have the intersection of their boundaries containing a segment of Y of positive length, which is impossible since the discs are distinct and have radius $r < 1$. Compactness of Z then shows that Y is isolated. \square

Definition 53. *Given a disc D and an integer $n \geq 3$, let D^n denote a smallest (unique up to rotation) regular n -sided polygon (with sides consisting of arcs of great circles) containing D , and similarly D_n the largest such polygon contained in D . Note that if D has algebraic centre, then D_n and D^n have algebraic vertices.*

Given a finite set of algebraic points S , set

$$(154) \quad U(S) = \{B_r(p) : p \in S\},$$

$$(155) \quad U_n(S) = \{(B_r(p))_n : p \in S\},$$

$$(156) \quad U^n(S) = \{(B_r(p))^n : p \in S\}.$$

Lemma 54. *Given a finite set S of algebraic points, the following hold:*

- 1) *if $U(S)$ is not a cover, and the complement of $U(S)$ has no isolated points, then there exists $n > 0$ such that $U^n(S)$ is not a cover.*
- 2) *if $U(S)$ is a cover, then there exists $n > 0$ such that $U_n(S)$ is a cover.*

Proof. 1) If $U(S)$ misses a point, then it misses an open set, in particular a disc of some radius $\epsilon > 0$. Eventually, the sets D^n for $D \in U(S)$ will have diameter less than $2r + \epsilon/4$, and so $U^n(S)$ will miss an open set of points.

2) this is clear by a similar argument, once we observe that given any cover of a compact set X by open sets $\{U_i\}_i$, there exists some $\epsilon > 0$ such that for every point $p \in X$ there exists an index i such that

$$(157) \quad B_\epsilon(p) \subset U_i.$$

\square

Proposition 55. *Given a finite set S of algebraic points and an integer $n \geq 1$, there exists an algorithm to determine whether $U^n(S)$ is a cover, and to determine whether $U_n(S)$ is a cover.*

Proof. It suffices to give an algorithm which, when given a finite set of polygons (with arcs of great circles as their sides), will determine whether these cover S^2 . This is easy; one approach is to subdivide the union of the polygons into a finite set of triangles which meet properly, then to compute the homology of the resulting complex; we have a cover if and only if the second homology group is non-zero. \square

Proposition 56. *Fix B a finite set of points in S^2 , and choose a rational number $0 < r < 1$ less than half of the shortest distance between two distinct points in B . Then Algorithm 57 will yield a finite cover C of S^2 by discs of radius r satisfying the following properties:*

- a) B is contained in the set of centres of discs in C ;
- b) Given a disc D in C and a point $p \in D$ which is the centre of a disc in C , then p must be the centre of D ;
- c) there exists a computable $\epsilon > 0$ such that for all p, q centres of discs in C , $d(p, q) \geq r + \epsilon$ (equivalently, property (1) still holds when the discs are replaced by their closures).

Algorithm 57. 1) Set $S = B$;

2) Set $N = 1$, and $m_1 = 1$;

3) for $1 \leq n \leq N$:

if $U_{m_n}(S)$ is a cover, output S , finish;

else if $U^{m_n}(S)$ is not a cover, use Proposition 51 to find an algebraic point $p_{(N,n)}$ outside $U^{m_n}(S)$ such that the complement of $U(S \cup \{p_{(N,n)}\})$ has no isolated points;

else $m_n + := 1$;

4) $N + := 1$, $m_N := 1$. Go to (2);

Proof. It is not hard to see that if the procedure terminates then the resulting cover has the desired properties, but it remains to prove termination. We argue this by contradiction; suppose that the procedure does not terminate. This yields a cover of S^2 by $U(S)$ for some infinite set of algebraic points S , so by compactness there exists a finite subset $T \subset S$ such that $U(T)$ is a cover. Let $N_0 > 0$ be such that

$$(158) \quad T \subset B \cup \{p_{(l,n)} : l \leq n \leq N_0\}$$

By Lemma 54, there exists $n_0 \geq 1$ such that $U_{n_0}(T)$ is a cover, and so the algorithm will terminate when $N = N_0 + n_0$. \square

REFERENCES

- [And02] G.W. Anderson. Edited 4-theta embeddings of jacobians. *Arxiv preprint math/0209413*, 2002.
- [BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [BMS⁺08] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and Sz. Tengely. Integral points on hyperelliptic curves. *Algebra and Number Theory*, 2:859–885, 2008.

- [Bru06] P. Bruin. Green functions on riemann surfaces and an application to arakelov theory. Master's thesis, Universiteit Leiden, 2006.
- [CE⁺11] J.M. Couveignes, B. Edixhoven, et al. Computational aspects of modular forms and galois representations. 2011.
- [CGO84] Vincent Cossart, Jean Giraud, and Ulrich Orbanz. *Resolution of surface singularities*, volume 1101 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1984. With an appendix by H. Hironaka.
- [CPS06] J. E. Cremona, M. Prickett, and Samir Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.
- [Dem68] V. A. Dem'janenko. An estimate of the remainder term in Tate's formula. *Mat. Zametki*, 3:271–278, 1968.
- [dJ04] R. de Jong. *Explicit Arakelov Geometry*. PhD thesis, Universiteit Leiden, 2004.
- [DJ05] R. De Jong. Arakelov invariants of riemann surfaces. *Documenta Mathematica*, 10:311–329, 2005.
- [DP02] S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes ii. *Commentarii Mathematici Helvetici*, 77(4):639–700, 2002.
- [Fal84] G. Faltings. Calculus on arithmetic surfaces. *The Annals of Mathematics*, 119(2):387–424, 1984.
- [Fly93] E. V. Flynn. The group law on the Jacobian of a curve of genus 2. *J. Reine Angew. Math.*, 439:45–69, 1993.
- [FS97] E. V. Flynn and N. P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, 79(4):333–352, 1997.
- [Hol12a] D. Holmes. Computing Néron-Tate heights of points on hyperelliptic Jacobians. *Journal of Number Theory*, 132(6):1295 – 1305, 2012.
- [Hol12b] D. Holmes. *Néron-Tate heights on the Jacobians of high-genus hyperelliptic curves*. PhD thesis, University of Warwick, 2012.
- [Hri83] P. Hriljac. The Néron-tate height and intersection theory on arithmetic surfaces. *PhD Thesis, Massachusetts Institute of Technology*, 1983.
- [Jav12] A. Javanpeykar. Polynomial bounds for arakelov invariants of curves with given belyi degree. *Preprint*, 2012.
- [Lan83] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.
- [Lan88] S. Lang. *Introduction to Arakelov theory*. Springer, 1988.
- [Liu02] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Ern , Oxford Science Publications.
- [Man71] Ju. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.
- [Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.
- [Mue10] J. S. Mueller. Canonical heights on Jacobians. 2010. Universit t Bayreuth PhD thesis.
- [Mue11] Mueller, J. S. Computing canonical heights using arithmetic intersection theory. *ArXiv e-prints, to appear in Math. Comp.*, May 2011.
- [Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.
- [Mum83] D. Mumford. *Tata lectures on theta I*. Birkh user, 1983.
- [N r65] A. N ron. Quasi-fonctions et hauteurs sur les vari t s ab liennes. *Annals of Mathematics*, 82(2):249–331, 1965.
- [Pen55] R. Penrose. A generalized inverse for matrices. *Proc. Cambridge Philos. Soc.*, 51:406–413, 1955.
- [Rei72] M. Reid. *The complete intersection of two or more quadrics*. PhD thesis, University of Cambridge, 1972.
- [Sik95] S. Siksek. Infinite descent on elliptic curves. *Rocky Mountain Journal of Mathematics*, 25(4), 1995.

- [Sil90] Joseph H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.
- [Sto99] M. Stoll. On the height constant for curves of genus two. *Acta Arith*, 90(2):183–201, 1999.
- [Sto02] M. Stoll. On the height constant for curves of genus two, ii. *Acta Arith*, 104(2):165–182, 2002.
- [Sto12] M. Stoll. Explicit kummer varieties for hyperelliptic curves of genus 3. 2012.
- [Uch06] Y. Uchida. On the difference between the ordinary height and the canonical height on elliptic curves. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 82(3):56–60, 2006.
- [VW98] P. Van Wamelen. Equations for the jacobian of a hyperelliptic curve. *Trans. Amer. Math. Soc.*, 350:3083–3106, 1998.
- [Zim76] Horst Günter Zimmer. On the difference of the Weil height and the Néron-Tate height. *Math. Z.*, 147(1):35–51, 1976.
- [ZM72] Ju. G. Zarhin and Ju. I. Manin. Height on families of abelian varieties. *Mat. Sb. (N.S.)*, 89(131):171–181, 349, 1972.